AN ABSTRACT OF THE THESIS OF

Turgay Caglar for the degree of Master of Science in Computer Science presented on June 15, 2021.

Title: An Approach to Help End Users Become Aware of Privacy Risks in Home Automation

Abstract approved:

____

Anita Sarma

Smart home devices, such as voice assistants, smart lights, and smart video doorbells have become a part of end users' daily lives. Many of these devices combine their features with other services and smart devices to create a simple and efficient user experience. This is partly because of the contribution of end-user programming platforms, like If This Then That (IFTTT). IFTTT provides trigger and action events to end users to connect two or more smart home devices via easy-to-create applets. However, these applets rarely highlight underlying risks related to confidentiality (leakage of sensitive information) or integrity (authorized access) violations.

Prior work has shown that providing users with violation scenarios makes them aware of the risks associated with these specific applets. However, these works have not investigated if end users can identify potential risks from the applet descriptions and change their behavior. This thesis closes this gap by (1) presenting end users with "consequences" of using IFTTT applets to understand if end users could find the possible violations and their reasoning, and (2) evaluating whether end users' behavior changes when applets are presented with the consequences. In this work, we conducted a user study with 20 participants to evaluate our approach of

including consequences in applet description. Our results show that adding potential consequences into the basic IFTTT applet description can help end users discover integrity and confidentiality violations and related factors impacting their applet usage decisions. Finally, we suggest a framework to automatically nudge end users when they want to use applets through end-user programming platforms. In this way, end users can have a comprehensive understanding of using applets in different contexts.

An Approach to Help End Users Become Aware of Privacy Risks in Home Automation

by

Turgay Caglar

A THESIS

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of

Master of Science

Presented June 15, 2021
Commencement June 2022

Master of Science thesis of Turgay Caglar presented on June 15, 2021

APPROVED:

Major Professor, representing Computer Science

Head of the School of Electrical Engineering and Computer Science

Dean of the Graduate School

I understand that my thesis will become part of the permanent collection of Oregon State University libraries. My signature below authorizes release of my thesis to any reader upon request.

Turgay Caglar, Author

ACKNOWLEDGEMENTS

I would like to express the most profound appreciation to my advisor, Dr. Anita Sarma and Dr. Rakesh Bobba. Without their supervision, this thesis would not have been possible.

I am incredibly grateful to my parents for their everlasting support. It is my privilege to thank my brother, Turgut Caglar, for his endless encouragement throughout my life.

I would also like to extend my gratitude to my committee members Dr. Mike Bailey and Dr. Leonard Coop.

My thanks and appreciations also go to all my friends who have gladly helped me out with their love.

CONTRIBUTION OF AUTHORS

Marjan Adeli helped with data analysis. Dr. Anita Sarma provided overall research direction and support. Dr. Rakesh Bobba helped with the study design and feedback on research.

TABLE OF CONTENTS

LIST OF FIGURES

<u>Figure</u> <u>Page</u>

LIST OF TABLES

Chapter 1: Introduction

Smart home devices, such as voice assistants, smart lights, and smart video doorbells, have become a part of end users' daily lives. Many of these devices combine their features with other services and smart devices to create a simple and efficient user experience. This is thanks, in part, to the contribution of end-user programming platforms, like If This Then That (IFTTT) [1], that allow users to connect devices and services very easily. These connected devices and services in IFTTT are called applets. Applets are built on the basic principle that an event selected as a trigger causes an action. Such applets are popularly used and shared among end users. The popularity of using and creating applets should not be surprising since creating and using applets does not require high-level technical skills; instead, one only needs to have access to services and IoT devices [2].

IFTTT provides specific trigger and action events to end users to give them an overall idea about applets' functionality. End users can create their applets with the help of the structure provided by IFTTT [3]. For example, an end-user can visit IFTTT website [1] to design or reuse an applet to connect voice assistants (e.g., Alexa) to smart lights. The user can turn on the lights (action) with a voice command (trigger) given to Alexa. These IFTTT applets can be used as-is from the available options on the platform or be reused from the examples that are on the IFTTT website. In 2020, there were 90 million applets running with 18 million users [4].

However, while these applets provide convenience and allow end users flexibility and an easy way to connect their smart devices, there are underlying risk (or often called violations) related to integrity and confidentiality. An integrity violation can occur when unintended users can trigger applets. Previously, we gave an example applet for Alexa and Light. For instance, when guests can trigger a voice assistant (e.g., Alexa) to turn on the smart lights, this can be an example of an integrity violation (assuming guests are not intended users who can trigger the applet). A confidentiality violation occurs when unintended users can observe the actions of the applets. For example, If guests can observe the smart lights, this can be an example of a confidentiality violation (assuming they are not planning to see the lights are on).

The context in which these applets are used can impact the risks. For example, the location of the smart assistant (e.g., Alexa) is important for the applets because unintended users can ask Alexa to trigger the event (unintended user). Therefore, the location of trigger devices affects integrity violations. Like other studies showed (e.g., [5][6] [7]), other risks can emerge based on contextual factors such as time of the day, location of trigger device, location of action device, and people at home. Contextual factors, like who can use the device, who is around, and trigger location, etc., can make users more cognizant of their privacy and security. These contextual factors are dependent on specific use scenarios.

However, end users may have a hard time figuring out possible violations. Especially, given that IFTTT has been designed for end users who do not need to have technical or security backgrounds. Many of these violations can occur in usage scenarios that are edge cases or those that arise when the different use cases have not been comprehensively thought through. This is especially true because the IFTTT applets often have sparse descriptions. This when combined with end users' limited ability to perform risk assessment makes this a significant problem for end users. For example, Alexa's location (trigger location) at home determines the possible people who can communicate with Alexa (who can use). If Alexa is in the kitchen while there are guests at home, the guests can also turn on/off the smart lights in any room using Alexa. In IFTTT, users can only see the trigger-action event within the description; privacy and security information about adopting applets may be missing. For this reason, conceiving possible usage scenarios that users did not initially have in mind helps them to shape their usage behavior to have a more overarching awareness of violations. The insufficient applet descriptions provided in IFTTT and users' limited prediction capabilities, when it comes to risk assessment, users may not be aware of the possible risks they may face while using applets, as stated in previous work [8]. Because of this, they may not envision potential negative consequences of using such applets, such as integrity and confidentiality violations.

Even though prior works have shown that violations can easily occur in the IFTTT domain, some studies were limited to access control or authentication in home automation [5, 9] . Other studies only [10, 11, 12] investigated users' privacy concern in IFTTT applets rather than the factors that influences end users' applet usage or reasoning. Prior work [5] has also shown that giving violation scenarios can prevent end users from taking risky actions, such as integrity and confidentiality violations. However, these scenarios did not highlight to what extent context factors can influence end users' applet usage. These studies in the field of home automation have only focused on users' concerns [6, 10, 13] instead of evaluating whether end users' behavior changes for their applets in different usage context.

While these are the first steps to understand how the context of use can affect confidentiality and integrity violation, we still do not know whether and how users' behavior would change for future applet usage or if they are aware of the consequences in applets that may lead to confidentiality and integrity violation. To close this gap, my thesis aims to understand end users' behaviors through the following Research Questions:

RQ1: What factors do end users consider when deciding to use an applet?

RQ2: How does presenting consequences of using an applet affect users?

RQ2a: To what extent do they consider other factors about applets with consequences?

RQ2b: To what extent does their behavior change for the applets with consequences?

RQ3: To what extent does seeing consequences influence the factors that users consider when evaluating an applet?

Research Question (RQ1) helps us create a baseline for us to understand which factors do end users consider when deciding to use an applet. While RQ1 provides us an understanding of the factors that end users consider when reading an applet description, RQ2a gives us insight into how adding consequences in applet descriptions can affect the factors that end users think about when deciding to use (or not use) an applet. RQ2b investigates the impact of presenting consequences (in a specific) applet on users' behavior in using other applets. Finally, RQ3 shows us if adding consequence in applet description influences the factors that users consider when evaluating an applet with only description. More specifically, my thesis goal is how adding consequences into applet description affects users' perception of their current and future applet usage.

To answer the research questions and reach my thesis goal, in this work, we designed a user study with 20 end users. This IRB approved study, included 3 main stages. Where in Stage 1, we showed participants applets with descriptions (pre-treatment). Then in Stage 2, we included consequences into description for specific applets to learn how the factors that influence their applets usage change (treatment). In Stage 3, we investigated the effect of the consequences on applets with description (post-treatment) In this user study, the participants were asked questions on eight different applets.

My results indicate that adding the possible consequences into the basic IFTTT applet descriptions can help end users discover integrity and confidentiality violations and related factors impacting their applet usage decisions. Thanks to the consequences in applet descriptions, participants could notice different usage scenarios in changing home environments to consider privacy-related factors when deciding to use or not to use applets. Additionally, our participants could change their applet usage behavior with more privacy-aware decisions in different usage contexts.

The overall structure of this thesis takes the form of six chapters, including this introductory chapter. In the second chapter, we provide a review of previous work related to this study. The third chapter presents the methodology used for this study. The fourth chapter is concerned with the findings of the research. Chapter five demonstrates how our results relate to i) assisting end users to think comprehensively in home automation ii) Nudge users for more privacy-aware decisions. Finally, chapter six provides the summary of the study with takeaways.

Chapter 2: Related Work

In this chapter, we present the related work. There are two subchapters for this reason that show how previous work has addressed: 1) Context in the IoT Environment 2) Preventing users from risky action

2.1 Context in the IoT environment

Much of the current literature on the IoT environment pays particular attention to contextual factors. Emami-Naeini et al. [12] studied users' comfort levels with different scenarios and contextual factors. This study was aimed at IoT devices where data collection occurs. They found that users are more comfortable with data collection happening in public places than in private places.

The study conducted by He et al. [5] explored users' preference on access-control points of single IoT devices. They investigated which contextual factors have an impact on users' choice for access-control specification. They found that users expect to have some control over access-control specification with contextual factors (e.g., location of the device, age of the people who can use the device) to create their desired usage environment. Lee and Kobsa [10] conducted a survey with different scenarios to understand how users' perception of IoT scenarios gets affected by contextual factors. They revealed four clusters for the scenarios based on users' reactions (acceptable, somewhat unacceptable, unacceptable, and very unacceptable). The relationship between these clusters and associated contextual factors showed that “what” (values: location, voice, etc.) and “who” (values: friend, colleague, etc.) are the two contextual factors that are key to determining clusters. Psychoula et al. [13] created different scenarios for their participants to capture the factors that impacted end users' privacy concerns. However, this study was limited to data collection in the IoT environment.

A recent study conducted by Saeidi et al. [6] relates most closely to ours regarding contextual factors presented in the study. They investigated how users' concerns change based on contextual factors in applet descriptions with a within-subject survey design. First, they created a baseline to see how the basic applet description contributes to users' concerns. Then, in the same survey, they asked participants how their concern would be based on given contextual factors with applet description. They found that contextual factors can raise users' concerns for the applets.

Another recent study conducted by Cobb et al. [14] investigated the potential risk of applets. They recruited 28 participants and asked them questions about installed applets. They found that participants were not concerned about potential negative outcomes of the applets even though they were explained. Moreover, they highlighted that end users could not be aware of people who can observe applet usage, like neighbors, friends, etc. Another important contribution in this study was that they updated previous security lattices [7] with some modifications.

Our work investigated how users' behaviors change based on given contextual factors and consequences rather than trying to interpret only users' concern. Instead of focusing on IoT devices, we focused on applets and their usage situations in the home. Although users have higher privacy concerns about using such applets in usage scenarios, we still do not know how these concerns affect users' decisions to use applets. Contextual factors that affect users' concerns can provide useful insight for both end users and security experts. However, the interpretation of why users' concerns increase (or why we expect them to increase) and how end users react in some scenarios is still unclear (whether it affects users' applet usage decisions or not). Therefore, instead of focusing on users' privacy concerns, we focused on users' applet usage decision changes and factors influencing their applet usage.

2.2 Preventing users from risky action

In terms of investigating users' behavior towards risky action in the IoT environment, Emami-Naeini et al. [15] interviewed 24 participants to understand users' IoT device purchase behavior better. They reported interviewees were less concerned about their privacy and security before purchase but more after the purchase because of news, feedback from friends, or unexpected device function. Features and price were the two most important factors that affected their decision; privacy and security came afterward. In the same study, researchers also suggested a label design for IoT devices. Their suggested label design encouraged users to be more aware of their IoT purchase decisions regarding privacy and security.

Besides IFTTT, there are other platforms where end users can use applets. SmartThings [16], HomeKit [17], and Zapier [18] are other examples of popular platforms. Fernandes et al. evaluated SmartThings and found some issues related to its design where applet creation and adoption occur [19]. By analyzing the existing applets, they revealed that most users have applets that require more permission than they need. As a result, they provided their learnings as a step towards a more secure home automation environment. Chiang et al. [20] conducted an empirical study to understand end users' behavior in IFTTT. They found that, among the most popular 500 applets in IFTTT, 91% of their trigger events have potential privacy leakage. They suggested some systems that can help end users securely manage their privacy in trigger-action platforms to solve this problem. Lekakis et al. [21] offered solutions for the data leakage that could occur in the home environment. The study aimed to provide solutions for confidentiality violations due to different home environments with roommates, family members, friends, etc. In this study, factors were only related to people who could share the home environment.

Fernandes et al. [22] proposed a system called FlowFence to give users more efficient control over their information flow. It enables users to protect their information flow by limiting unintended trigger events. In the smart home domain, Zhen et al. [23] conducted semi-structured interviews with 11 end users for eight different households to investigate end users' privacy perceptions. They found that users can trade their privacy over convenience since they think that the IoT device companies protected their data. Also, they stated that users do not change the configuration of devices they have after they start using. Therefore, they highlighted the importance of better nudging and configuration systems for IoT devices.

Celik et al. proposed IoTGuard [24] system to prevent users from experiencing integrity and confidentiality violations. They determined some applet policies for their study and tested them with a set of IoT devices and apps. They showed that IoTGuard could block risky actions when integrity or confidentiality violations might happen. Another study has been conducted by Bastys et al. [25] to prevent users from confidentiality, integrity, and availability violations by developing an automated tool. Similarly, other past research has also shown that some systems can help users from risky actions like sensitive data flow or unintended information flow control. For example, SAINT [26] identifies sensitive information flow in application codes. SmartAuth [27] allows users to understand potential problems like unintended app authorization that can be missing in applet descriptions. ContexIoT [28] provides efficient access control to users for their sensitive actions like intended information flow.

Previous works studied various types of nudge designs in different domains such as software installation, password creation, and posting in SNS, social network services. The purpose of these nudges was to prevent users from risky actions when they were required to make decisions like posting pictures on social media or changing passwords for their applications.

For example, Masaki et al. [29] explored how different nudges help users assess risk better in social network services. They designed 11 different nudges and nine scenarios for their survey. They found users are more likely to avoid risky choices when presented with negatively worded nudges (e.g., 20% of people wouldn't post this picture without permission.). Zimmermann and Renaud investigated nudges in cybersecurity-specific decisions [30]. They performed an empirical study to see which types of nudges (simple, information, or hybrid) can be more effective when users need to make cybersecurity-related decisions (choice of cloud service, password creation, smartphone encryption, and choice of public Wi-Fi). They found hybrid nudges, a combination of simple and information nudges, were as effective as simple nudges to help users make more secure choices in cybersecurity.

By definition [31], nudges aim to help users make safer decisions about risky user actions without taking away their freedom of choice. Users make these risky decisions at obvious decision points (whether to post friends' pictures without permission or not). On the other hand, the decision to purchase an IoT device is also a clear decision point for end users (purchase or not purchase). However, decision points are not clear for applets because the routine is established once the end user adopts a specific trigger-action event.

In the IoT environment, even though end users do not interact with the services or devices, they may need to make decisions about their privacy and security (whether they would use the applets or not) due to the occurrence of contextual factors and related consequences in usage situations. Therefore, our work provides valuable insight on devising appropriate decision points to “nudge” users to more privacy-aware behaviors when they have applets in different contexts.

Chapter 3: Methodology

In this chapter, we present our user study methodology. We conducted our user study with 20 participants to understand what factors influence end users' applet usage.

We managed the study via Zoom (a video conference tool), one-on-one with individual participants to understand their reasoning for the factors that may affect their applet usage.

In past works, researchers have conducted surveys on Mechanical Turk, an online platform that allows researchers to find participants for their studies [6, 12, 15]. However, a survey leaves gaps in our understanding because we cannot ask participants follow-up questions where needed. Therefore, we chose the in-person study format. The following subsections explain our methodology in detail.

3.1 Recruitment and screening

Our participants were required to use or have used at least one IoT applet to be eligible for the study. These screening criteria allowed us to efficiently present our applet selection since they already had experience with IoT applets.

After we got IRB approval, we emailed students at Oregon State University to find participants. Our email included our screening criteria. Our pilot user studies showed us participating user study was between 35-40 min. Therefore, we compensated participants with an Amazon gift card worth $20.00.

3.2 Participants

We recruited 20 participants for our user study via the university mailing list. Table 1 shows the demographics of the participants. We had 11 men and nine women in our study. Twelve participants were in the 25-34 age group, and 8 participants were 18-

24. Most of the participants (16 participants) had a bachelor's degree. There was 1 participant with a doctorate, 1 participant with a high school degree, and 2 participants with a master's degree. Most of our participants had 1 or 2 IFTTT applets (17 participants), 2 participants had 3 to 4 applets, and 1 participant had more than four applets.

Table 1: Demographics of participants

Par.[i]	Gen.[ii]	Age[iii]	Edu.[iv]	IFTTT[v]	Par.[i]	Gen.[ii]	Age[iii]	Edu.[iv]	IFTTT[v]
P1	M	25-34	M	1-2	P11	W	25-34	B	1-2
P2	M	25-34	M	1-2	P12	M	25-34	B	1-2
P3	W	18-24	B	1-2	P13	W	25-34	B	1-2
P4	M	25-34	B	1-2	P14	M	18-24	B	1-2
P5	W	18-24	H	5+	P15	M	18-24	B	1-2
P6	W	18-24	B	1-2	P16	M	18-24	B	1-2
P7	W	25-34	B	1-2	P17	M	18-24	B	3-4
P8	M	25-34	B	1-2	P18	W	18-24	B	1-2
P9	W	25-34	B	1-2	P19	M	25-34	B	1-2
P10	M	25-34	D	3-4	P20	W	25-34	B	1-2

[i]Participant (e.g., P1 for Participant 1) [ii] Gender (M for Male, F for Female) [iii] Age of participants [iv]Education level of participants (H for high school, B for bachelors, M for masters and D for doctorate) [v] Number of IFTTT applets that participants have

3.3 Study design

Our key study goal was to investigate the impact of showing end users the consequence of using an applet in a specific usage context, which was the treatment in our study.

3.3.1 Applets and consequences

To decide which applets to have in the user study, we focused on the most frequently adopted applets from the IFTTT dataset published by Ur et al. [32] . Two researchers discussed the most frequent applets and decided not to include applets 1) if they are similar to each other in terms of trigger action event (e.g., Alexa-smart TV applet "to turn on" and "to turn off") 2) if they are not directly related to the home environment (e.g., location-twitter applet " to post a tweet whenever users enter a location". Next, to limit the user study time and see if our applets and consequences have meaning for our participants, we conducted a formative study with our research team. After the formative study, we decided on keeping the top 8 applets after previous requirements have met. Our formative study with more information is in the next section: pilot study.

Since we did not have a similar format for each applet in our dataset, we decided to have a general applet description design. We wanted to emphasize applets' essential functions: trigger and action events. Besides, we wanted to have one general usage example for each applet we have. For example, one of the Alexa - Smart Light (Hue) applet descriptions in IFTTT is "Turn your hue lights on by saying "Alexa, trigger lights on". For this specific applet, we came up with our description, which has a trigger-action event with one simple usage example:" There is an applet that connects your Alexa and Philips Hue lights. This specific applet will turn your lights on when you ask Alexa to "turn on lights''. In this example, our trigger event is asking Alexa to turn on the lights, and the action is lights being turned on. Thanks to this format, we could efficiently introduce our applets to our participants. This allowed our participants to focus on applets' possible usage scenarios. Table 2 presents all the applets we included in this study.

Table 2: Applets with descriptions

Applets	Tri.-Act.[i]	Description
App 1	Alexa - Spotify	Suppose there is an applet that connects your Voice Assistant (Alexa) to a music service app (Spotify). This specific applet will play your Spotify when you say "Alexa, play my Spotify top hit playlist".
App 2	Alexa - Light	Suppose there is an applet that connects your Voice Assistant (Alexa) and Smart Lighting (Philips Hue lights). This specific applet will turn your lights on when you ask Alexa to "turn on lights".
App 3	Alexa - TV	Suppose there is an applet that connects your Voice Assistant (Alexa) to your smart TV. This specific applet will turn your smart TV on when you ask Alexa to "turn on the TV".
App 4	Alexa - Evernote	Suppose there is an applet that connects your Voice Assistant (Alexa) to a note-taking app (Evernote). This specific applet will add items to your list when you say, "Alexa add milk to my grocery list".
App 5	Location - Light	Suppose there is an applet that connects your location information and Smart Lighting (Philips Hue lights). This specific applet will turn off all the lights when you leave a specific area.
App 6	SMS - Light	Suppose there is an applet that connects your Smart Lighting (Philips Hue lights) and SMS. This specific applet will blink your lights when you receive an SMS.
App 7	Thermostat - Email	Suppose there is an applet that connects your Smart thermostat (Nest thermostat) and your email. This specific applet will send you an email when your thermostat is set to away mode.
App 8	Fitness - Coffee Maker	Suppose there is an applet that connects your Fitness Tracker (Fitbit) and coffee maker. This specific applet turns your coffee maker on when your Fitbit logs that you have woken up for the day.

[i]Trigger - Action (e.g., Alexa is trigger, TV is action device for App 3)

In this study, our treatment was a possible consequence of using specific applets. Two researchers discussed the potential consequences and threat models of using the applets in the home environment. After considering different threat models for each applet we had, we decided to include possible outcomes based on the outstanding contextual factors. For instance, when we had Alexa as a trigger device in our applets, we agreed on having a consequence based on its location and who can use it (who can trigger the action). Finally, we categorized our applets based on the possible contextual factors that can cause end users to have negative outcomes. Our two main categories for the applets are 1) Trigger Location & Who can use (applet) 2) Action Location & Who is around (who can notice the action). For example, Applet 1 (Alexa-Spotify) is in the trigger Location & Who can use category. Therefore, we created the consequence by having a possible scenario with the location of Alexa (the kitchen was the trigger location) and who can use Alexa (guests were who can use). Also, we gave them one possible consequence for this scenario: guests could ask Alexa in the kitchen to listen to the songs in your playlist. Table 3 shows all applets with consequences.

Table 3: Applets with their categories and consequences

Applets	Tri.-Act.[i]	Cat.[ii]	Consequences
App 1	Alexa - Spotify	1	If you have guests, they can ask Alexa in the kitchen to listen to the songs in your playlists.
App 2	Alexa - Light	1	If you have guests, they are able to turn on your lights with Alexa in the kitchen for any room (kitchen, living room, bedrooms, etc.).
App 3	Alexa - TV	1	If you have guests, they are able to ask Alexa in the kitchen to turn on the TV in any room (kitchen, living room bedrooms, etc.).
App 4	Alexa - Evernote	1	If you have guests, they can ask Alexa in the kitchen to add some items to your grocery list.
App 5	Location - Light	2	If taxi service drivers (Uber) can infer you are not home when your lights located in your living room are off.
App 6	SMS - Light	2	If you have guests in your home and another friend is excited about a movie and is texting you, your friend can cause your lights, located in the hallway, to blink.
App 7	Thermostat - Email	2	If you are sharing your screen with your audience (coworkers, friends, etc.), they can see the e-mail notifications (subject, e-mail body, etc.) on the shared screen (Zoom, Google Meet, etc.) and infer when there is no one home.
App 8	Fitness-Coffee Maker	2	If you have guests, they can assume that you are sleeping when your coffee maker is not on in the kitchen.

[i]Trigger - Action (e.g., Alexa is trigger, Light is action device for App 2) [ii]Category names (Category 1 for trigger location and who can use, Category 2 for action location and who is around)

3.3.2 Pilot study

We conducted a pilot study to find answers to the following questions: 1) How much time our user study would take based on each applet we included in our study 2) How our applets descriptions and consequences would sound to the participants.

To find answers to these questions, we conducted a formative study with two participants in our research group. Our participants correctly explained what they understood from reading consequences and applet descriptions. Moreover, our pilot user studies showed us participating user study was between 35-40 min with eight applets. Therefore, we limited our study to eight applets.

3.3.3 Study protocol

At the start of the study, we collected participant demographics (gender, age, education, applet background) and current applets to determine their eligibility (screening criteria). Before we started our user study with our applet selection, we also asked them questions about the applets that they had, why they had them, the factors that they considered when our participants used them, and the concerns that they had with them. These questions let us find factors that they could consider with their current applets. We refer to this data as the Current Applet in the result chapter.

The study included two main Rounds. For each round, we presented five applets to our participants. Within each round, there were three stages.

Stage 1: **pre-treatment.** In this stage, we showed our participants an applet description and asked them 1) whether they would use the applet or not 2) factors they would consider when using (or not using) the applet. We refer to these applets as pre-treatment applets in the result chapter.

Stage 2: **treatment.** After the pre-treatment stage, we showed our participants the same applet with consequences and asked them the same questions as in pre-treatment 1) whether they would use the applet or not, 2) factors they would consider when using (or not using) the applet. We refer to these applets as treatment applets in the result chapter.

Stage 3: **post-treatment.** After the treatment stage, we showed them the description of 3 different applets. We asked the same questions as in pre-treatment and treatment stages: 1) whether they would use the applet or not, 2) factors they would consider when using (or not using) the applet. We refer to these applets as post-treatment applets in the result chapter.

We presented our applets one by one. For each applet, we repeated the questions according to their applet assignment (Table 5). If participants did not elaborate their answers or gave us short answers, we asked them follow-up questions: 1) When participants only mentioned the usefulness of applets, we asked them whether there was any other factor besides usefulness. 2) When participants gave us simple answers or factors without explaining why, we asked them why questions to learn their reasoning. 3) If participants said, "Yes, I would use this applet " and gave us no explanation for the previous follow-up questions as well, we asked them whether they would have any concerns using the applet.

We recorded the audio for each participant and transcribed them. We used transcriptions for qualitative analysis discussed in the Result section.

3.3.4 Order of the applets in the study

We wanted to minimize the carry-over effects; therefore, we counterbalanced the order in which participants experienced an applet such that:

Each of the eight applets in the study should be in pre-treatment and a post-treatment experiment run. We counterbalanced the order in which the rounds were presented. Half of the participants experience Category 1 applets first (App 1, App 2, App 3, App 4) and Category 2 applets second (App 5, App 6, App 7, App 8) and vice versa.

First, we created four different applet groups (Table 4) to present our eight applets in different orders. We randomly assigned each participant to each applet group. We designed our study so that each participant had two treatments (possible consequence) for two different applet groups (Category 1 and 2 applets).

Table 4: Grouping of applets

Groups[i]	Part.[ii]	Category 1 Applets[iii]	Category 2 Applets[iv]
Group 1	5	App 1, app 1*, app 2, app 3, app 4	App 5, app 5* , app 6, app 7,app 8
Group 2	5	App 2, app 2*, app1, app 4, app 3	App 6, app 6*, app 5, app 8, app 7
Group 3	5	App 3, app 3*, app 4, app 1, app 2	App 7, app 7*, app 8, app 6, app 5
Group 4	5	App 4, app 4*, app 3 ,app 2, app 1	App 8, app 8*, app 7 , app 5, app 6

[i]Applet Groups [ii] Number of participants assigned to the group [iii] Category 1 Applets (trigger location and who can use), [iv]Category 2 Applets (action location and who is around) , *applets with consequences (treatment)

We recruited five participants for each group we had in Table 4. Table 5 shows the final assignment of all participants (n=20). As we can see in Table 5, to reduce the carry-over effect that could occur because of the order of the applets, half of the participants experienced Category 1 applets first (App 1, App 2, App 3, App 4) and Category 2 applets second (App 5, App 6, App 7, App 8) and vice versa. Therefore, we could present all our applets as pre-treatment (before presenting applets with consequence), treatment (presenting applets with consequence), and post-treatment (presenting applets without consequence after presenting them with consequence). For example, Participant P1 was in Group 1; therefore, in Round 1, he experienced Category 1 first. Then in Round 2, he experienced category 2 applets. Table 2 and Table 3 show applets with their description and consequences (treatment).

Table 5: Participant and assigned applet categories for the first and second round

Par.[i]	Par. Grp.[ii]	First Round[iii]	Second Round[v]	Par.[i]	Par. Grp.[ii]	First Round[iii]	Second Round[v]
P1	1	Category 1	Category 2	P11	3	Category 1	Category 2
P2	1	Category 2	Category 1	P12	3	Category 2	Category 1
P3	1	Category 1	Category 2	P13	3	Category 1	Category 2
P4	1	Category 2	Category 1	P14	3	Category 2	Category 1
P5	1	Category 1	Category 2	P15	3	Category 1	Category 2
P6	2	Category 1	Category 2	P16	4	Category 1	Category 2
P7	2	Category 2	Category 1	P17	4	Category 2	Category 1
P8	2	Category 1	Category 2	P18	4	Category 1	Category 2
P9	2	Category 2	Category 1	P19	4	Category 2	Category 1
P10	2	Category 1	Category 2	P20	4	Category 1	Category 2

[i]Participant (e.g. P1 for Participant 1) [ii] Participant Group [iii] First round experience (e.g. P2 received Category 2 applets in the first round) [iv]Second round experience (e.g. P4 experienced Category 1 applets in the second round)

3.4 Data analysis

Each participant recording was first transcribed, and then we segmented our user study data based on answers we collected for the applets. These transcriptions were then qualitatively coded. The primary purpose of qualitative coding in this research was to identify the factors that participants could consider when deciding to use or not to use applets. One of the researchers was the primary coder, responsible for creating and updating the codebook. We performed inductive coding for our data.

The primary coder conducted open coding with 5% of the segmented data (randomly selected) to develop the initial codebook. Then, two researchers independently coded 5% of the data for each round. At the first round, the inter-rater reliability (IRR - Cohen’s Kappa [33]) was 0.6 (moderate agreement). We then discussed how to solve disagreements in the code and continued the process. At the end of round four, our codebook was stabilized with high inter-rater reliability

(Cohen's κ =0.91) [33]. After we agreed on the codebook, two researchers coded half of the rest of the data individually. The final codebook is in Appendix A.

Chapter 4: Results

We present our results in this section structured as per our research questions. As we stated before, we have three main Research Questions:

RQ1: What factors do end users consider when deciding to use an applet?

RQ2: How does presenting consequences of using an applet affect users:

RQ2a: To what extent do they consider other factors about applets with consequences?

RQ2b: To what extent does their behavior change for the applets with consequences?

RQ3: To what extent does seeing consequences influence the factors that users consider when evaluating an applet.

4.1 Users' concerns before consequences

As we presented in our Methodology Chapter (Study Protocol), we had three stages for our user study. Stage 1 included the applets before we presented applets with consequences. We refer to these applets as pre-treatment applets.

Our Research Question 1 (RQ1) investigated the factors in the pre-treatment applets (before showing consequences).

RQ1. What factors do end users consider when deciding to use an applet?

Our RQ1 goal was to draw a baseline understanding of what factors end users could consider for applet usage. Therefore, this RQ1 provided us insight into IFTTT basic applets and how they sounded to our participants.

At the beginning of the user study, our participants talked about their current applets. In our main user study, we had three stages. In Stage 1, we had applets with descriptions (pre-treatment applets). Table 6 shows the factors (codes) we captured with current and pre-treatment applets. The first column is a combination of these two. Participants identified 17 factors.

When we considered current and pre-treatment applets together, convenience was the most dominant factor influencing users' decisions (37% of all codes). All our participants (n=20) found pre-treatment applets convenient.

The factors related to the “desire-to-use applets” were “convenience” (20 participants cited), "interesting" (four participants cited) , "environmental benefits" (4 participants cited), "high tech" (three participants cited), and "showing off" (two participants cited). There were two factors related to cost: "cost of using" applets (five participants cited) and "cost of buying" applets (one participant cited). Only three participants cited "privacy" (3% of all codes) and one participant cited "safety" (1% of all codes) as a factor directly.

Since the coverage of the codes decreases dramatically, we want to introduce the top 5 applets from each table. Appendix A has all factors (codes) with definitions and examples.

Convenience. All the participants (n=20) mentioned convenience as a factor for the pre-treatment applets. Participants think that applets are useful and make their life easier. As one participant said (Participant 16): *"I'm using this applet because it's making my life easier. I can turn on my lights without using a physical switch. "*. Another participant said (Participant 6): *“It makes my life easier. Because I can turn on my television with my voice comment.”*

Table 6: Codes (factors) that we captured for current and pre-treatment applets

		Total			Current Applets			Pre-treatment Applets		
Index	Codes	Tot.Obs. i	Cov. ii	Uniq. iii	Tot.Obs. i	Cov. ii	Uniq. iii	Tot.Obs. i	Cov. ii	Uniq. iii
1	convenience	**44**	**37%**	**20**	20	49%	20	24	30%	19
2	consistency	**24**	**20%**	**14**	8	20%	8	16	20%	12
3	unauthorized access (3)	**10**	**8%**	**7**	6	15%	6	4	5%	4
4	restriction for trigger	**7**	**6%**	**5**	0	0%	0	7	9%	5
5	cost of using	**5**	**4%**	**4**	1	2%	1	4	5%	4
6	undesired outcome	**5**	**4%**	**5**	1	2%	1	4	5%	4
7	interesting	**4**	**3%**	**4**	2	5%	2	2	3%	2
8	privacy	**4**	**3%**	**3**	1	2%	1	3	4%	2
9	environmental benefits	**4**	**3%**	**4**	0	0%	0	4	5%	4
10	high tech	**3**	**3%**	**3**	0	0%	0	3	4%	3
11	showing off	**3**	**3%**	**3**	0	0%	0	3	4%	3
12	who can trigger	**2**	**2%**	**2**	0	0%	0	2	3%	2
13	who can observe (action)	**1**	**1%**	**1**	1	2%	1	0	0%	0
14	who can observe (trigger)	**1**	**1%**	**1**	1	2%	1	0	0%	0
15	cost of buying	**1**	**1%**	**1**	0	0%	0	1	1%	1
16	safety	**1**	**1%**	**1**	0	0%	0	1	1%	1
17	unauthorized access (U)	**1**	**1%**	**1**	0	0%	0	1	1%	1

[i]Total Observation for the codes (e.g., we coded convenience 20 times in current applet section: middle column, index 1) [ii] Coverage of the code (e.g., for pre-treatment applets (last column) consistency (index 2) covers 20% of all codes) [iii] number of unique participant (e.g., 5 different participant mentioned about restriction for trigger (index 4) in pre-treatment applets (last column))

Consistency. Almost 20% (Table 6, index 2, first column) of codes were about the consistency of devices and applets. Fourteen participants mentioned that sometimes applets or devices did not work as expected. For example, Participant 11 mentioned this problem: " *...sometimes Alexa misunderstands me. Sometimes it can have issues with understanding.*"

Unauthorized Access (3). Seven participants were worried about whether their data was collected by unknown third parties or companies of the devices (8% coverage: Table 6, index 3, first column). For instance, Participant 20 said: *" When I say Alexa, it hears. So, it can also listen to my other talks."*

Restriction for trigger. Five of our participants mentioned restrictions for the trigger devices (6% coverage: Table 6, index 4, first column). Some of them wanted to restrict people who can trigger the applet. For example, one participant (Participant 17) was worried about the trigger for Applet 4 (Alexa-Evernote): *"Sometimes we are just thinking loudly, and it is not a good idea to write everything whatever we say."*

Cost of using. Four of our participants highlighted the cost of using applets (4% coverage: Table 6, index 5, first column). Participant 18 said (for Applet 8, Fitbit-Coffee maker): *"I do think that it would be a waste of energy, and I am trying to keep utility bills down where we're pretty strict about leaving stuff on or turning stuff on when it's not being used."*

Undesired outcome. Five participants complained about undesired outcomes of using applets (4% coverage: Table 6, index 6, first column). Some participants were worried about unexpected applet behavior. For Applet 8 (Fitbit-Coffee Maker), Participant 12 also said: *"I am always getting up grabbing water using the bathroom or just lying awake. And so, I think that it would just be constantly turning it on."*

In total (for current, pre-treatment, treatment, and post-treatment applets), we came up with 21 unique factors that influence users' applet usage (Appendix A). However, participants only mentioned 17 of them before giving them applets with treatments (consequences). Factors that no participants mentioned in this section (4 out of 21 factors): location of action, location of trigger, health, and disturbing other.

4.2 Effect of applets with consequences on users' concern and decision to use applets

Our second research question was (RQ2): How does presenting consequences of using an applet affect users? We divided this research question into two parts:

RQ2a. To what extent do they consider other factors about applets with consequences?

RQ2b. To what extent does their decision to use applets change for the applets with consequences?

4.2.1 Effect of applets with consequences on users' concern

In this subchapter, we present the factors we discovered for the treatment applets (applets with consequences).

RQ2a. Our goal with RQ2a was to investigate how factors affecting users' applet usage could change based on consequences (treatment).

As we can see in Table 7, we have only 12 factors for treatment applets. Participants cited fewer factors for treatment applets (12 factors) than pre-treatment applets (17 factors). Since our treatment had consequences for particular usage contexts, participants were mainly focused on privacy and confidentiality violations.

Privacy was the most cited factor (17 participants cited) influencing users' decisions (18% of all codes). 13 participants cited "who can observe (action)," which is also related to privacy.

The factors related to the "privacy" were "who can observe (action)" (13 participants cited), "who can trigger" (12 participants cited) , "restriction for trigger" (eight participants cited), "unauthorized access (3)" (five participants cited), "location of trigger" (five participants cited), "unauthorized access (U)" (four participants cited), “who can observe (trigger)” (two participants cited). Moreover, 10 participants cited “safety” as a factor.

Participants did not mention the following factors for the treatment applets: "high tech", "showing off", "location of action", "interesting", "cost of buying", "cost of using", "consistency", "environmental benefits”, and "health". This was likely because participants were more concerned about confidentiality and integrity violations than the desire-to-use and cost-related factors. Since we created usage scenarios with adding consequences into applet descriptions, our participants cited the factors related to specific use cases. Table 7 shows all the consequences for eight applets.

"Privacy" as a factor had the most influence on our participants for the treatment applets. Seventeen participants mentioned privacy. "Who can observe (action) " was the second most frequent factor in this section (13 participants cited). These factors are related to each other because if unintended people can observe the action event, this leads to confidentiality violation. "Who can trigger" was the third most frequent factor cited by 12 different participants. This factor is directly related to authorized users, which impacts whether it is an integrity violation or not. Also, eight participants cited “restriction for trigger” as a factor to mention that IoT devices need to allow applet owners to decide who can access trigger events (e.g., Alexa). Similar to these factors, safety was the fourth most frequent factor for our participants (10 participants cited).

Like in Table 6, the coverage of the factors decreases dramatically for the treatment applets (Table 7). Therefore, we present the five most frequently cited factors for Table 7. Since "restriction for trigger" was in the previous table's five most frequently cited factors (Table 6), we did not repeat the same factor.

Table 7: Codes (Factors) that we captured for applets with treatments

		Treatment		
Index	**Codes**	**Tot.Obs.** [i]	**Cov.** [ii]	**Uniq.** [iii]
1	privacy	21	18%	17
2	who can observe (action)	19	16%	13
3	who can trigger	16	14%	12
4	safety	11	9%	10
5	restriction for trigger	10	9%	8
6	undesired outcome	8	7%	7
7	disturbing other	6	5%	5
8	unauthorized access (3)	6	5%	5
9	location of trigger	6	5%	5
10	unauthorized access (U)	5	4%	4
11	convenience	4	3%	4
12	who can observer (trigger)	4	3%	2

[i]Total Observation for the codes (e.g., we coded privacy 21 times in treatment applet section: index 1) [ii] Coverage of the code (e.g., for treatment applets who can observe (action) (index 2) covers 16% of all codes) [iii] number of unique participant (e.g., 12 different participants mentioned who can trigger (index 3, last column))

Privacy. Seventeen participants were worried about their privacy for the applets with consequences (18% coverage: Table 7, index 1). For instance, Participant 4 commented on App 5 with the consequence (Table 5): " *It breaks my privacy.* So I wouldn't want to be known from the outside. It's uncomfortable.". The same participant also said (App 1): *"So maybe you don't want them to know your personality at that moment. Maybe you want the be the leader of these devices. They shouldn't have access to your devices."*

Who can observe (action). 13 participants mentioned "who can observe the action event" as a factor that influenced their applet usage (16% coverage: Table 7, index 2). Most of them also figured out the connection between who can observe (action) and privacy factors. For app 7 (thermostat-email), participant 11 said: *"People watching my screen can know when exactly I'm in the house.."*

Who can trigger. Twelve participants mentioned that who can trigger the applet could influence their applet usage (14% coverage: Table 7, index 3). Participant 17 did not want his guests to add items to his grocery list (App 4 with consequence): "*In my house, I would like to take all the controls. I really respect my guests, but they don't understand it. This is my house, and this is my grocery list.*"

Safety. 10 participants mentioned safety as a factor (9% coverage: Table 7, index 4). For Applet 5 (location-light), Participant 1 said: "*When I leave home, I always turn on at least one light because people should think that I am home because of a theft situation, burglary, or something like that.* "

4.2.2 Effect of applets with consequences on users' decision to use applets.

As we previously mentioned, our second research question was (RQ2): "How does presenting consequences of using an applet affect users?" This research question has two parts. Here we discuss second part:

RQ2b. To what extent does their decision to use applets change for the applets with consequences?

In the study, we asked our participants, "Would you use this applet" for each applet to learn how their usage behavior would change based on the different usage contexts we created (consequences). Therefore, we could see whether their decision to use applets changed (RQ2b) based on our consequences (treatment).

Table 8 presents if our participant's decision has changed based on the consequence in the applet description or not. Seventeen participants reversed their decision to use applets because of their privacy and safety concerns. Green highlighted rows in Table 8 represent these 16 participants. For example, one participant stated (P11) like this for applet 5 (location-light) before introducing her to the same applet with a consequence: *"I like this one. I think I would use this because I always forget to turn off the lights. My roommates are angry because of this. ".* The same participant (P11), when asked the same applet with the consequence, said: *"I wouldn't use it. I think this is not safe. Also, I don't want anyone to know if I am home or not. If they know this information they can steal something."*

Table 8: Yes (I would use this applet) and No (I would not use this applet) answers of participants for the pre-treatment and treatment applets

Participant ID	Pre-treatment Decision	Treatment decision	Participant ID	Pre-treatment Decision	Treatment decision
1	Yes	No	11	Yes	No
2	Yes	No	12	Yes	No
3	Yes	Yes	13	Yes	Yes
4	Yes	No	14	Yes	No
5	Yes	No	15	Yes	Yes
6	Yes	No	16	Yes	No
7	Yes	No	17	Yes	No
8	No	No	18	Yes	No
9	Yes	No	19	Yes	No
10	Yes	No	20	Yes	No

As shown in Table 8, three participants (yellow highlighted) did not change their decision not to use the applets with consequences. There were two reasons for this: 1) Participant 13 trusted people "who can observe the action" 2) Participant 3 and Participant 15 still wanted to use applets with consequences due to the usefulness of the applets. Participants 13 and 15 did not think it would be a big problem for them to use the applets with the consequences. On the other hand, we can explain Participant 13's reasoning with a lattice model. For example, Participant 13 said:

"I would trust anyone who is looking at my screen would be someone who I would trust with that kind of information. Any coworkers or friends, I trust that they would not rob my house knowing that I wasn't there."

She might have responded like this because this was happening in a restricted physical environment, like shown in previous work [7]. Because of this, she might think that people (who can observe action) in this environment could be trustable for her.

Participant 8 (highlighted blue) was the only one who said: "*I wouldn't use this applet*" for both pre-treatment and treatment applets. He did not see any purpose in using app 6 (SMS-Light). He said: " *I don't know why people would use this. I don't think this applet is helpful.*"

These findings show that we need to assist end users in understanding the possible consequences of using applets in changing home environments. This helps their decision to use (or not to use) applets with a more comprehensive understanding. Therefore, we present the carry-over effect of consequences presented in the applet description in the following subchapter.

4.3 Carry-over effects of the consequence on users' concern

As we mentioned before, our user study had three stages. The third stage had the applets we presented to our users after applets with consequences (post-treatment applets). Therefore, the results we present in this subchapter collected from the applets presented in third stage, which were post-treatment applets (applets after consequences have shown).

Our third research question was (RQ3): To what extent does seeing consequences influence the factors that users consider when evaluating an applet? This research question aimed to understand how adding consequences into applet description (treatment) affected users' understanding of evaluating an applet with the only basic description (post-treatment). Therefore, in this result subchapter, we investigate the carryover effects of the consequence in the applet descriptions.

RQ3. To what extent does seeing consequences influence the factors that users consider when evaluating an applet?

We present the factors we discovered for the post-treatment applets (applets shown after consequences) in Table 9. As we can see in Table 9, we have 21 factors for the post-treatment applets, which were all the factors we discovered in our user study. We presented our post-treatment applet to participants with only applet descriptions after the treatment (consequences in applet description). However, participants cited more factors for post-treatment applets than pre-treatment (17 factors) and treatment applets (12 factors).

"Convenience" was the most cited factor (20 participants cited) influencing users as a factor when they were evaluating the applet whether to use or not (22% of all codes). The other factors we captured for "desire-to-use" applet categories were "interesting" (12 participants cited, 3% of all codes), " high tech" (six participants cited, 2% of all codes, "showing off" (five participants cited, 1% of all codes.),and "environmental benefits" (3 participants cited, 1% of all codes). We listed all code categories in Appendix B.

"Privacy" was the second most cited factor as a concern among our participants (16 participants cited, 14% of all codes)

Table 9: Codes (Factors) that we captured after applets with treatments (post-treatment)

		post -treatment		
Index	**Codes**	**Tot.Obs. [i]**	**Cov.[ii]**	**Uniq.[iii]**
1	convenience	78	22%	20
2	privacy	49	14%	16
3	who can trigger	37	10%	15
4	who can observe (action)	35	10%	14
5	undesired outcome	32	9%	14
6	location of trigger	20	6%	10
7	consistency	19	5%	10
8	restriction for trigger	15	4%	11
9	unauthorized access (U)	13	4%	6
10	disturbing other	11	3%	6
11	interesting	12	3%	6
12	high tech	6	2%	6
13	location of action	5	1%	5
14	unauthorized access (3)	5	1%	5
15	showing off	5	1%	5
16	cost of using	4	1%	3
17	cost of buying	4	1%	3
18	environmental benefits	3	1%	3
19	safety	3	1%	3
20	health	2	1%	2
21	who can observer (trigger)	2	1%	2

[i]Total Observation for the codes (e.g., we coded convenience 78 times after applets with treatments (index 1)) [ii] Coverage of the code (e.g., for the post-treatment applets, privacy (index 2) covers 14% of all codes) [iii] number of unique participant (e.g., 15 different participants mentioned who can trigger (index 3, last column))

"Who can trigger" was the third most frequently cited factor for post-treatment applets (15 participants cited, 10% of all codes). This factor is directly related to integrity violation since it decides whether it is authorized or unauthorized access. We categorized this factor under "integrity/confidentiality related contextual factors," as seen in Appendix B. In this category, we also had other factors cited by our participants: "who can observe (action)" (14 participants cited, 10% of all codes), "location of trigger" (10 participants cited, 6% of all codes), "unauthorized access (U)" (six participants cited, 4% of all codes), "location of action" (five participants cited, 1% of all codes), "unauthorized access (3)" (five participants cited, 1% of all codes), and "who can observe (trigger)" (two participants cited, 1% of all codes).

Our participants were also concerned about "undesired applet/device performance". The fourth most frequently cited factor for post-treatment applets was "undesired outcome" (14 participants cited, 9% of all codes). The other factors related to this category were: "consistency" (10 participants cited, 5% of all codes) and "disturbing others" (6 participants cited, 3% of all codes).

Participants also mentioned cost-related factors for applets or IoT devices. We captured two factors for this category: "cost of using" (three participants cited, 1% of all codes) and "cost of buying" (three participants cited, 1% of all codes).

Three participants were concerned about "safety" for post-treatment applets (1% of all codes). Additionally, only two participants cited "health" as a factor(1% of all codes).

As shown in Table 9, all participants (n=20) cited “convenience” because their main focus was the promised usage scenario. Fourteen participants cited “Undesired outcome” as a factor since it was the concern of the participants about applet behavior, which was also related to the promised usage scenario. On the other hand, in the top 5 most frequently cited factors for post-treatment applets, we had "privacy, "who can trigger", and "who can observe (action)" as a concern among our participants. Participants were worried about their "privacy" because, for the treatment applets (applets with consequences), they experienced some specific scenarios where privacy-related issues could occur. Therefore, they carried over this awareness to the post-treatment applets. "Who can trigger" an applet is an important factor because integrity violation occurs when an unintended user ("who can trigger") can trigger an applet. Furthermore, "who can observe (action)" is also important because confidentiality violation occurs if an unintended user ("who can observe (action)") can witness the action event of an applet (lights are on/off, a coffee maker is working or not, etc.).

Figure 1 presents the top five most frequently cited factors with their coverage for the pre-treatment, treatment, and post-treatment applets. Hence, Figure 1 shows the summary of previous tables.

As we can see in Figure 1, convenience was the most dominant factor for the pre-treatment and post-treatment applets. Both had something in common: these applets only had basic IFTTT descriptions. At first glance, participants were primarily curious about if the applets were helpful or not (worth using or not). Additionally, "undesired outcome" was also a common factor for the pre-treatment and post-treatment applets. Privacy was the primary concern for applets with consequences. However, for pre-treatment applets, coverage of privacy was only 3%. This shows that adding consequences into basic applet descriptions can help people think about privacy-related factors. Besides, "who can trigger" and "who can observe (action)" were two factors that were also related to privacy as participant 16 cited for Applet 6 (SMS-Light): "*Privacy is so important for me. I definitely don't want to inform my girlfriend [who can observe (action)] when I receive the SMS*". These two factors were in the top five most frequently cited factors list for treatment and post-treatment applets.

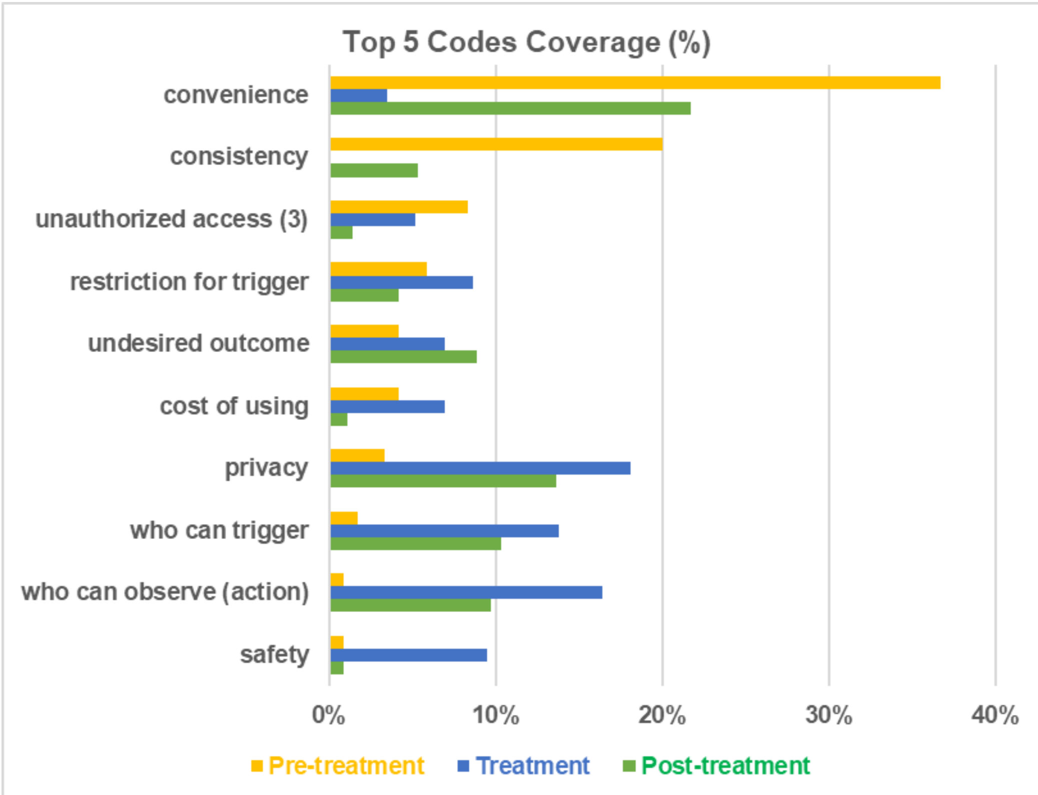

Figure 1: The top five most frequently cited codes (factor) coverage for the pre-treatment, treatment, and post-treatment applets

This result also confirms that our consequence had a carry-over effect on our participants' understanding of applet usage. Even though we presented only applet descriptions after we gave them our applets with consequences (treatment), they could still think of the factors related to confidentiality and integrity violations. However, since applet's descriptions highlighted the primary trigger-action event with simple examples of use, they also cited factors related to desire-to-use applets.

Chapter 5: Discussion

In this chapter, we discuss the results which relate to 1) assisting end users to think comprehensively in home automation 2) nudge users for more privacy-aware decisions: automated tools.

5.1 Assist end users to think comprehensively about home automation

Our study showed that IFTTT descriptions are not enough for end users to think comprehensively (RQ1). They miss privacy-related factors that they could consider. The factors that our participant cited with basic applet description were mostly about desire-to-use applets ("convenience", "environmental benefits", "high tech", "interesting", and "showing off"), applet/device working performance ("consistency" , "undesired outcome", and "disturb others") or data collection by third-party companies ("unauthorized access (3)"). Previous work [34] has also shown that applet owners may have incorrect expectations for their home automation. They may think the home is private and safe; therefore, they might miss likely-to-happen integrity and confidentiality violations. End users' focus could be on the promised usefulness of applets with basic descriptions.

In this study, our treatment had consequences in applet description. Once participants received the treatment, they also highlighted the contextual factors investigated in previous work [10]. For example, who can observe (action) and who can trigger were the main factors for some studies, (e.g., [6, 14]) which affected confidentiality and integrity violations. Previous work (e.g., [6, 35]) also highlighted the importance of “restriction for trigger” while investigating the user concerns with applets in IFTTT. Therefore, our findings align with previous work as well. Importantly, our work leverages prior studies to determine the other factors that influence end users' applet usage.

Since we had only the applet descriptions for our post-treatment applets, users focused on the applets' functionality to decide if they would use it or not. However, participants still had some concern for the post-treatment applets. "Who can observe (action) " and "who can trigger" were two factors we captured in the top five most frequently cited factors for post-treatment applets. "Who can observe (action)" may lead to confidentiality violation since unintended users can observe the actions of the applets. Additionally, "who can trigger" may lead to integrity violation since unintended users can trigger the applets. These two factors are also related to "privacy," which was also in the top five most frequently cited factors. Since the applets we picked were suitable for the home environment, the same user could use all IoT devices connected. Therefore, "who can trigger" (related to integrity violation) and "who can observe" (related to confidentiality violation) could have the same meaning in most cases. Since a user who can trigger the applet can also observe the action, this circumstance raised privacy concerns among our participants. Hence, this confers that adding consequences in applet descriptions can help users think comprehensively when deciding to use applets.

As discussed earlier in the Related Work chapter, nudges aim to help users make safer decisions about risky user actions [17], like creating passwords or posting pictures on social media, without taking away their freedom of choice. Unlike these, it is not clear for end users when they need to make decisions for their applets in their home environment. When end users set up their applets for their home automation, they configure and use them with some factors that they had in their mind. However, the home is a living environment. For example, people who are living at home or are visiting the home can affect this environment. Therefore, end users need to notice when the decision points in the home environment occur.

5.2 Nudge end users towards making privacy-aware decisions with automated tools

These findings have significant implication opportunities for developing automated tools to nudge users for more privacy-aware decisions. All the contextual factors have a different meaning for each applet. We could only include eight applets in our study. Therefore, we wanted to demonstrate a tool which can generate consequences with eight applets we included in our study.

We developed an initial tool that could produce consequences based on the selection of contextual factors (trigger/action location and "who can be at home with applet owner"). Figure 1 shows the interface of the tool. In this tool, the applets were limited to the ones we included in this study. The tool currently uses pre-generated consequences across a selection of the applets used in our study and some contextual factors. The tool then provides drop-down selection options for the users and presents the appropriate consequence, as shown in Figure 2.

Future Implications. We initiated creating an automated consequence generator with the applets we included in this study. However, a further study with more applets is needed to develop a fully automated consequence generator. For example, for end-user programming platforms, a browser extension could be helpful for the end users. When end users want to connect devices, an extension can pop up to show the related consequences for that applet. This kind of nudging mechanism can help end users think of other scenarios that they could face in the home environment. Therefore, such a tool can help end users create a comprehensive understanding of using applets in different contexts.

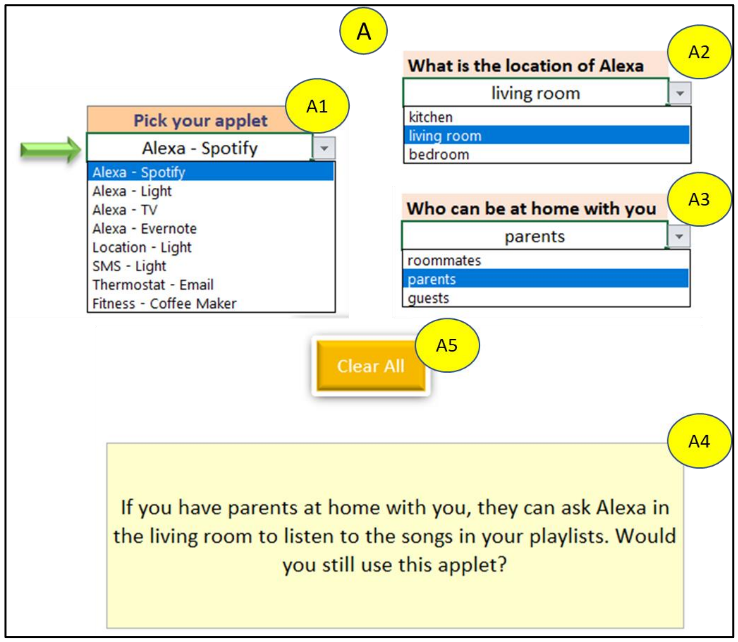

Figure 2: Consequence Generator

Consequence generator interface (A) with the components of applet selection (A1), “location of trigger/action” selection (A2), “ can be at home with applet owner” selection (A3), generated consequence based on selections (A4), and a button to clear selected fields (A5)

5.3 Threats to validity

Like every other study, we have some limitations in this user study. Although our participants had at least one applet because of our screening criteria, we could find our participants through the university mailing list. Our participants were mostly in the 25-34 age group, and they had at least a high school degree. Therefore, we likely could not discover all the factors that have an influence on their applet usage since end users, in general, are more diverse.

We performed inductive coding in this study. Therefore, the codes we captured in the study could be subjective. However, we tried to avoid this threat by discussing our findings with our research group to reach an agreement.

We had two rounds in our study, and in each round, we had one pre-treatment, one treatment, and three post-treatment applets. Each of the eight applets in the study presented in a treatment and a post-treatment position. We also counterbalanced the order of the rounds. Half of the participants experience category 1 applets first (App 1, App 2, App 3, App 4) and Category 2 applets second (App 5, App 6, App 7, App 8) and vice versa.

However, as in any user study our results cannot be fully generalized to all populations or applets. Since we had to limit our study time, we could include only eight applets in our study. There are so many applets with different functionalities. In end-user programming platforms like IFTTT, eight applets are a small set of the whole universe. However, we picked the most popular applets and combined their similar futures. Therefore, our applet selection was not unusual for our participants.

Chapter 6: Conclusion

In this thesis, we conducted a user study with 20 participants to understand: (1) what factors influence end users' applet usage, (2) how presenting consequences of applet use affects users' concerns and decision making in applet usage, and (3) the carry-over effects of the consequence on users' concern. We captured 21 factors that influenced users' applet usage. Moreover, the factors in this study, which impacted their applet usage decisions, also expand on previous research, where only predetermined factors have been investigated.

We conducted our user study in three stages: 1) pre-treatment stage (before applets with consequences), 2) treatment stage (applets with consequences) 3) post-treatment stage (after consequences have shown).

We found that basic applet descriptions were not enough for our participants to see integrity and confidentiality violations in different usage contexts. These findings come from our pre-treatment applets. Since applets had promised usage scenarios with basic trigger and action events, users focused on its functionality. Therefore, the factors that our participant cited mostly about desire-to-use applets.

Moreover, our work showed that adding consequences into basic applet descriptions can help users think more comprehensively regarding integrity and confidentiality violations in different usage contexts. For treatment applets(applets with consequences), the most cited factors were related to confidentiality and integrity violations as well as users' privacy. Additionally, users' decision to use the specific applet changed after they were shown the applet with consequences.

For example, 17 participants said: " Yes, I would use this applet" before consequences have shown to them (pre-treatment). However, they changed their answer to "No, I wouldn't use this applet" when they were shown the consequences about that applet. Therefore, adding consequences into basic applet descriptions can help users make privacy-aware decisions in different usage contexts.

To see the carry-over effect of showing consequences on users' understanding of privacy and security concerns when they evaluate other applets, we showed our participants different applets with basic descriptions after showing the applet with the consequence (post-treatment). Users remained mainly focused on the applet's usefulness since basic applet descriptions had promised functionality (trigger-action event). However, our participants cited integrity ("who can trigger") and confidentiality ("who can observe(action)") related factors more frequently than in the pre-treatment stage. Additionally, they could find the connection between these factors and reasons about their "privacy" concerns. Therefore, adding consequences into basic applet descriptions can help people understand potential violations that could occur in different usage contexts.

In summary, our work has also shown that users are more aware of their security and privacy with the help of consequences in applet descriptions. Adding consequences into basic applet descriptions can prevent users from integrity and confidentiality violations. We created a basic prototype which can generate consequences for a set of IFTTT applets. A future step would be creating an automated consequence generator based on Natural Language Processing of the applet descriptions along with the choice of context factors selected by the end user. Such automated tools, created as browser extensions, could nudge end users when they are planning to connect their devices in end-user programming platforms by giving them a more comprehensive understanding of different usage scenarios.

Bibliography

[1] If This Then That (IFTTT), https://ifttt.com/ (accessed February 15, 2021).

[2] Ovadia S. Automate the Internet With “If This Then That” (IFTTT). *Behavioral & Social Sciences Librarian* 2014; 33: 208–211.

[3] Johnson D. What is IFTTT?, https://www.businessinsider.com/what-is-ifttt (2021, accessed April 13, 2021).

[4] 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 May 31, 2021).

[5] He W, Golla M, Padhi R, et al. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In: *27th {USENIX} Security Symposium ({USENIX} Security 18)*. 2018, pp. 255–272.

[6] Saeidi M, Calvert M, Au AW, et al. If This Context Then That Concern: Exploring users’ concerns with IFTTT applets. *Arxiv*.

[7] Surbatovich M, Aljuraidan J, Bauer L, et al. 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, WWW ’17*. 2017, pp. 1501–1510.

[8] Zeng E, Mare S, Roesner F. End User Security and Privacy Concerns with Smart Homes. In: *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*. 2017, pp. 65–80.

[9] Mazurek ML, Arsenault JP, Bresee J, et al. Access control for home data sharing: : Attitudes, Needs and Practices. *Proc 28th Int Conf Hum Factors Comput Syst - Chi ’10* 2010; 645–654.

[10] Lee H, Kobsa A. Understanding User Privacy in Internet of Things Environments. *2016 IEEE 3rd World Forum Internet Things Wf-iot* 2016; 407–412.

[11] Lee H, Kobsa A. Privacy Preference Modeling and Prediction in a Simulated Campuswide IoT Environment. *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)* 2017; 276–285.

[12] Naeini PE, Bhagavatula S, Habib H, et al. Privacy Expectations and Preferences in an IoT World. In: Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017). 2017, pp. 399–412.

[13] Psychoula I, Singh D, Chen L, et al. Users' Privacy Concerns in IoT Based Applications. IEEE 2018; 1887–1894.

[14] Cobb C, Surbatovich M, Kawakami A, et al. How Risky Are Real Users' IFTTT Applets? In: *Sixteenth Symposium on Usable Privacy and Security ({SOUPS} 2020)*. 2020, pp. 505–529.

[15] Emami-Naeini P, Dixon H, Agarwal Y, et al. Exploring how privacy and security factor into IoT device purchase behavior. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* 2019; 1–12
.

[16] SmartThings, https://www.smartthings.com/ (accessed April 12, 2021).

[17] HomeKit, https://www.apple.com/ios/home/ (accessed April 12, 2021).

[18] Zapier, https://zapier.com/ (n.d., accessed April 12, 2021).

[19] Fernandes E, Jung J, Prakash A. Security Analysis of Emerging Smart Home Applications. In: *2016 IEEE symposium on security and privacy (SP)*. 2016, pp. 636–654.

[20] Chiang Y-H, Hsiao H-C, Yu C-M, et al. On the Privacy Risks of Compromised Trigger-Action Platforms. In: *European Symposium on Research in Computer Security*. 2020, pp. 251–271.

[21] Lekakis V, Basagalar Y, Keleher P. Don't Trust Your Roommate or Access Control and Replication Protocols in "Home" Environments. In: *Proceedings of the 4th USENIX conference on Hot Topics in Storage and File Systems*. 2012.

[22] Fernandes E, Paupore J, Rahmati A, et al. Flowfence: Practical data protection for emerging iot application frameworks. In: *25th USENIX Security Symposium (USENIX Security 16)*. 2016, pp. 531–548.

[23] Zheng S, Apthorpe N, Chetty M, et al. User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction* 2018; 1–20.

[24] Celik ZB, Tan G, McDaniel P. IoTGuard: Dynamic Enforcement of Security and Safety Policy in Commodity IoT. In: *NDSS*. 2019.

[25] Bastys I, Balliu M, Sabelfeld A. If This Then What?: Controlling Flows in IoT Apps. In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 2018, pp. 1102–1119.

[26] Celik ZB, Babun L, Sikder AK, et al. Sensitive Information Tracking in Commodity IoT. In: 27th {USENIX} Security Symposium ({USENIX} Security 18). 2018, pp. 1687–1704.

[27] Tian Y, Zhang N, Lin Y-H, et al. SmartAuth: User-Centered Authorization for the Internet of Things. In: *26th {USENIX} Security Symposium ({USENIX} Security 17)*. 2017, pp. 361–378.

[28] Jia YJ, Chen QA, Wang S, et al. ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms. In: NDSS. 2017.

[29] Masaki H, Shibata K, Hoshino S, et al. 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*. 2020, pp. 1–11.

[30] Zimmermann V, Renaud K. The Nudge Puzzle: Matching Nudge Interventions to Cybersecurity Decisions. *ACM Transactions on Computer-Human Interaction (TOCHI)* 2021; 28: 1–45.

[31] Thaler RH. Nudge, not sludge. *American Association for the Advancement of Science*.

[32] Ur B, McManus E, Ho MPY, et al. Practical trigger-action programming in the smart home. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2014, pp. 803–812.

[33] McHugh ML. Interrater reliability: the kappa statistic. *Biochem Medica* 2012; 22: 276–282.

[34] Kaaz KJ, Hoffer A, Saeidi M, et al. Understanding user perceptions of privacy, and configuration challenges in home automation. In: *2017 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*. 2017, pp. 297–301.

[35] Corno F, Russis LD, Roffarello AM. A Semantic Web Approach to Simplifying Trigger-Action Programming in the IoT. Computer 2017; 50: 18–24.

APPENDICES

Appendix A: Codebook

#	Codes(Factors)	Definition	Examples
1	consistency	device problem, internet problem	sometimes Alexa misunderstands me
2	convenience	usefulness and easier to use, making life easier	It sounds very useful, it seems helpful.
3	cost of buying	price of applet/devices	is it worth spending money on it will spending money on it helped my life?
4	cost of using	increasing/decreasing my electricity bill	it's increasing my electricity bill
5	disturb others	when the applet functionality(trigger or action) disturbs other people	I can disturb my guests [sounds of coffee maker]
6	environmental benefits	saving earth, global warming, saving energy for the earth	like environmental friendly, maybe I can say energy efficiency or something like this,
7	health	affecting health	it can affect your health
8	high tech	modern technology	makes me feel that I'm living in the future because of the technology
9	Interesting	curiosity to new technology/applets	it sounds very cool.
10	location of action	where is action happening (kitchen, living room etc.)	the location of the lights if people can see them from that location
11	location of trigger	when they are talking about trigger device's location	if I use it [Alexa] in my room, it sounds cool, but if I use it in living room, maybe it won't.
12	privacy	access to information of applet owner	it threatens my privacy
13	restriction for trigger	voice recognition, only trigger in certain time of the day, confirmation to trigger applet	Fitbit could give me the option to make coffee and I could select yes or no
14	safety	robbery, stealing	it does not feel safe. They would rob my house
15	showing off	showing off	it can be a good way to showing off to your guests.
16	unauthorized access (3)	companies can listen to Alexa/ Alexa is listening to every conversation	I worry that Alexa is listening to my conversations and might be targeting ads for me
17	unauthorized access (U)	if someone is triggering/ seeing action to get information about applet owner	using this device, my friend or my guest can reach that, that list
18	undesired outcome	sending too many emails, blinking lights frequently	sometimes I'm waking up so early, but I'm going to turn back sleep [coffee machine works each time]
19	who can observe (trigger)	who can observe triggering (e.g., Alexa)	they [neighbors] can listen to me. They can hear what I am taking as a note
20	who can observe(action)	who can see the action of the applets	someone can read my personal notes
21	who can trigger	who can trigger(Alexa) the applet except applet owner	then any person can ask Alexa

Appendix B: Code (Factor) categories

Code (Factor) Category	**Code (Factor)**
cost	cost of buying
	cost of using
desire-to-use applets	convenience
	environmental benefits
	high tech
	Interesting
	showing off
health	health
integrity / confidentiality related contextual factors	location of action
	location of trigger
	unauthorized access (3)
	unauthorized access (U)
	who can observe (trigger)
	who can observe (action)
	who can trigger
privacy	privacy
restriction for trigger	restriction for trigger
safety	safety
undesired applet/device performance	consistency
	undesired outcome
	disturb others

Appendix C: Pre-generated consequences in Excel

Index	Applet	Final Conseqeunce (Column D+E + F + G + H + I)	Place holder 1	Place holder 2	Place holder 3	Place holder 4	Place holder 5
1	Alexa - Spotify	If you have at home with you, they can ask Alexa in the to listen to the songs in your playlists. Would you still use this applet?	If you have	(roommates/parents/ guests)	at home with you, they can ask Alexa in the	(kitchen/living room/ bedroom)	to listen to the songs in your playlists. Would you still use this applet?
2	Alexa - Light	If you have at home with you, they are able to turn on your lights with Alexa in the for any room (kitchen, living room, bedrooms, etc.). Would you still use this applet?	If you have	(roommates/parents/ guests)	at home with you, they are able to turn on your lights with Alexa in the	(kitchen/living room/ bedroom)	for any room (kitchen, living room, bedrooms, etc.). Would you still use this applet?
3	Alexa - TV	If you have at home with you, they are able to ask Alexa in the to turn on the TV in any room (kitchen, living room bedrooms, etc.). Would you still use this applet?	If you have	(roommates/parents/ guests)	at home with you, they are able to ask Alexa in the	(kitchen/living room/ bedroom)	to turn on the TV in any room (kitchen, living room bedrooms, etc.). Would you still use this applet?
4	Alexa - Evernote	If you have at home with you, they can ask Alexa in the to add some items to your grocery list. Would you still use this applet?	If you have	(roommates/parents/ guests)	at home with you, they can ask Alexa in the	(kitchen/living room/ bedroom)	to add some items to your grocery list. Would you still use this applet?
5	Location - Light	If taxi service drivers (Uber) can infer you are not home when your lights located in your are off. Would you still use this applet?	If taxi service drivers (Uber) can infer you are not home when your lights located in your			(kitchen/living room/ bedroom)	are off. Would you still use this applet?
6	SMS - Light	If you have at home with you, and another friend is excited about a movie and is texting you, your friend can cause your lights, located in , to blink. Would you still use this applet?	If you have	(roommates/parents/ guests)	at home with you, and another friend is excited about a movie and is texting you, your friend can cause your lights, located in	(kitchen/living room/ bedroom)	, to blink. Would you still use this applet?
7	Thermostat - Email	If you are sharing your screen with your audience (coworkers, friends, etc.), they can see the e-mail notifications (subject, e-mail body, etc.) on the shared screen (Zoom, Google Meet, etc.) and infer when there is no one home.					
8	Fitness - Coffee Maker	an assume that you are sleeping when your coffee maker is not on in	If you have	(roommates/parents/ guests)	at home with you, they can assume that you are sleeping when your coffee maker is not on in the	(kitchen/living room/ bedroom)	. Would you still use this applet?