Priming effects on Smarthome Users Choices while Managing Privacy

Paritosh Bahirat
School of Computing
Clemson University
pbahira@clemson.edu

Reza Ghaiumy Anarky
School of Computing
Clemson University
rghaium@clemson.edu

ABSTRACT

Smarthome IoT by it's nature, collects personal data through a web of several sensors present in the environment. Sometimes, the number of sources in a home can be overwhelmingly large and it can be challenging for the users to manage their privacy in such environments. A good way to present large number of In this paper, we present findings of study of part of an already developed *Privacy Management Interface*, showing various default profiles which a user can choose from. We also aim to gain an understanding of how users make their choices in presence of priming effect by leveraging eye tracking techniques.

KEYWORDS

Internet of Things, Privacy , Interface Design, Eye Tracking

1 INTRODUCTION

A study by PWC [11] , suggests that lower levels of Household IoT adoption are primarily due to high cost of ownership. Interestingly, the second-biggest reason of hesitation towards adoption is privacy and security concerns [11]. Arguably, such concerns may rise as costs decrease and adoption increases. Privacy is an inherent trade-off in IoT, because IoT devices cannot provide their services without collecting data. Moreover, many IoT devices provide personalized services, which requires them to retain and process the data as well. In some cases, users might regret making a bad disclosure decision and in some other cases they might not even be aware that a chunk of their data is being collected by a device. An unwanted disclosure can harm users' well-being negatively and also can cause dissatisfaction from system provider. Thus, it is important for IoT interfaces to help users make careful privacy decisions.

In this proposal we present an interface which was developed as a result of a survey study by [3] where they looked at several parameters in IoT privacy decision making context and how these impact the user decision making. We propose a user study on part of design Privacy Management Interface where we test how priming effects have an impact on the users choice of a profile. We apply eye tracking methodologies to understand how users look at our interface after they are shown different definitions of IoT technology.

We begin this article by exploring previous research done in privacy decision making literature. Then, we explain the methodology of our study while explaining the interface design (stimulus of eye tracking study) which we intend to show to the participants of our study, followed by various questions which will be asked from the participants. Then we put forward our hypotheses and discuss in detail the results of our study and what they point towards.

2 RELATED WORK

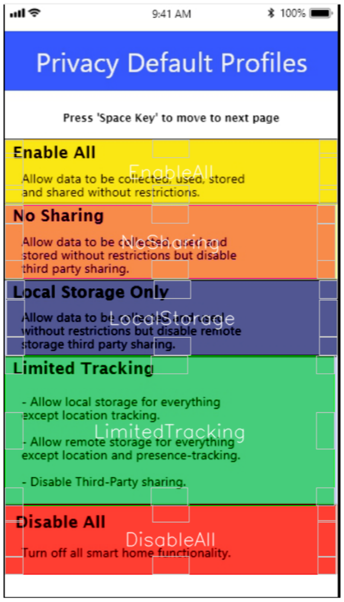
Privacy decision making is complex and it is a combination of several heuristics which range from default and framing effects to priming effects. Research proposes that users make a careful trade-off between risks to privacy and benefits from a service; a process often dubbed the "privacy calculus" [[5, 8]. Presentation of decisions itself has a strong impact on how users make decisions, according to Ariely, user decisions not just irrational but they are predictably irrational [2]. Framing effects were first investigated by Kahneman and Tversky [7], who explained them in terms of loss aversion: people have a higher tendency to avoid a loss than to pursue a gain. This would imply that people are more likely to consent to something when it is framed negatively than when it is framed positively. Framing and default effects may move users away from their "true preferences" [6], and such a deviation between users' true and selected preferences is likely to backfire. Finally, priming also has an effect on users' privacy decision making [10]. This has particularly been explored in case of social networking sites [10]. We intend to take this idea further and apply it in case of IoT Privacy decision making.

Use of Eye tracking studies has been extensively recommended to evaluate usability of systems [12]. Eye tracking methodologies have also been extended to investigate the privacy paradigms. Steinfeld conducted an interesting study to better understand how users read privacy notices [13]. However use of eye tracking to study privacy decisions in IoT domain has not been explored and we aim to fill this gap by taking a step in this direction.

3 METHODOLOGY

To explain the design of user study, we first begin with discussing the designed interface which we intend to test. This interface is a list of various profiles which were developed as a result of statistical and machine learning analysis of data collected by Bahirat et. al. [3] These profiles are part of a Smarthome Privacy Settings interface. Users can first select any of these profiles which they find most suitable for them. Users have an option to further micromanage the settings as well. However, for the scope of this study, we limit ourselves to how users interact with just the profiles interface (See Figure- 1). The profiles in the interface (See Figure- 1) range from

, ,
© 2016 Copyright held by the owner/author(s).
ACM ISBN 123-4567-24-567/08/06.
https://doi.org/10.475/123_4



9:41 AM 100%

Privacy Default Profiles

Press 'Space Key' to move to next page

Enable All

Allow data to be collected, used, stored and shared without restrictions.

No Sharing

Allow data to be collected, used and stored without restrictions but disable third party sharing.

Local Storage Only

Allow data to be collected and used without restrictions but disable remote storage third party sharing.

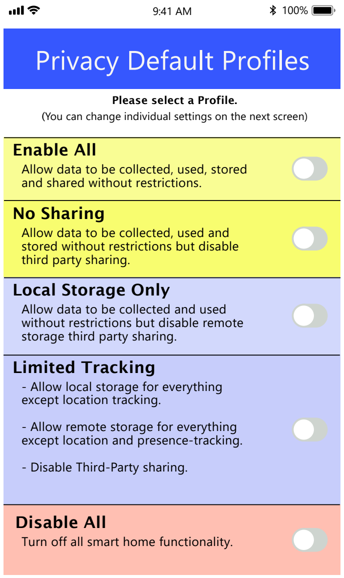
Limited Tracking

- Allow local storage for everything except location tracking.
- Allow remote storage for everything except location and presence-tracking.
- Disable Third-Party sharing.

Disable All

Turn off all smart home functionality.

Figure 1: Stimulus Interface with different profiles and example of different AOI (Areas of Interest)



9:41 AM 100%

Privacy Default Profiles

Please select a Profile.
(You can change individual settings on the next screen)

Enable All ○

Allow data to be collected, used, stored and shared without restrictions.

No Sharing ○

Allow data to be collected, used and stored without restrictions but disable third party sharing.

Local Storage Only ○

Allow data to be collected and used without restrictions but disable remote storage third party sharing.

Limited Tracking ○

- Allow local storage for everything except location tracking.
- Allow remote storage for everything except location and presence-tracking.
- Disable Third-Party sharing.

Disable All ○

Turn off all smart home functionality.

Figure 2: Stimulus Interface with profile selection button.

highly conservative (Disable all at the bottom) to highly liberal (Enable all at the top). In the rest of this section, we first explain the design of our user study where we highlight the independent variable. Then we detail other aspects such as participants, procedures, stimuli and so on for our user study.

3.1 Independent Variables

In this study we manipulate only one variable which is the text shown to participants before interacting with they interface. The participants were given either a positive (Benefit Focused) or a Negative (Privacy Concern Focused) text about IoT to read. This study follows a *Between Subject Design* with only one manipulation. This manipulation is discussed in detail in the subsequent sections of the paper.

As for the introduction text about IoT, a benefit focused introduction will positively prime the participants by providing a positive explanation of IoT smarthome environments. In this condition, we describe various benefits of using IoT technology such as conveniences and energy savings. On the other hand, the drawback focused introduction will be used to negatively prime participants with disadvantages in terms of privacy and data collection concerns of IoT environments. The exact positive and negative scenarios are discussed more in Table- 1

3.2 Apparatus

To collect participants eye movements and fixations, we used a Gazepoint GP3 pupil corneal reflection eye trackers. Per the manufacturer, the eye trackers are capable of an accuracy of one degree of visual angle with a 60 Hz sampling rate. The eye tracker will be used on a 22 inch Dell P2213 monitor screens having a resolution of 1680 x 1050.

3.3 Procedures And Stimulus

In the beginning of the study, the participants were informed about their role in this study, given instructions and the study began once they agreed to be a part of it upon reading the informed consent. The Gazepoint eye tracker was first calibrated for each participant. Next, participants were shown a brief introduction of Smart home IoT. This introduction was either benefit or drawback focused. This is the stage where participants were primed with experimental condition. After reading this introduction, participants visited Figure 3a. The purpose of this screen was to act as a buffer before the stimuli is presented. We then showed the participants our interface design (Figure- 1). After seeing the stimulus, the users visited Figure 3b which had instructions about what to expect in the next image. The image following figure 3b is shown at Figure 2 which is similar Figure 1 but only difference being is that it has buttons on the right side. We asked user to fixate on desired option and press "space" button. At this point, the eye tracking part of the study is finished.

3.4 Measurement

We developed a post-experiment survey. All participants filled out the survey after they finished the eye-tracking task. In this survey, we used previous items to measure users general knowledge about IOT technology, their privacy awareness [9], and general privacy concerns [9]. All items are measured by 7-point Likert scales and reported in Table 2. We ran CFA (confirmatory factor analysis) on these factors and reported the loading of each item. Unfortunately, due to the low number of participants we could not conduct further factorial analysis. We also used fixation per minute measured by Gazepoint software.

Table 1: Positive and Negative scenarios

Priming	Text
Positive	In today's Smarthome, one can expect to find all the appliances of a regular household. The only difference is that appliances in a Smarthome will be capable of various functionalities without needing human interference. These functionalities improve convenience of routine household activities and tasks. For example, a Smart Thermostat can detect presence of the person in the house by contacting Smartlock in the door. Then it can use this information to automate the temperature controls for home. Smarthomes are beneficial because they help in automating several day to day tasks without the occupant's intervention. This automation can also be helpful in energy savings and eventually reducing electricity costs. For example, a smart lighting system will automatically dim the lights based on existing natural light and also turn them ON/OFF based on occupants' presence.
Negative	Smarthomes comprise of several routine appliance found in an ordinary household. The key difference though is the additional functionality provided by these appliances. For example, a smart assistant in your home can order you a taxi in case of a bad weather. This convenience however comes at a cost. This cost is not only financial. The several devices in a smarthome environment with built in sensors heavily rely on collection of data from the owner or the people in these environments. The devices passively collect large amounts of data, whether a person is present inside home or not, what are the likes and dislikes of the people living in the smarthomes and so on. The devices not only share the data with different appliances in the home but can also share it with Manufacturers or third parties. This shared data can be used to give targeted advertisements and recommendations to you.

Table 2: Measurement items

Factor	Item	Loading
IOT knowledge 1	I know pretty much about smart home devices.	0.984
IOT knowledge 2	I do not feel very knowledgeable about smart home devices.	0.879
IOT knowledge 3	Among my circle of friends, I am one of the experts on smart home devices.	0.843
IOT knowledge 4	Compared to most other people, I know less about smart home devices.	0.718
IOT knowledge 5	When it comes to smart home devices, I really do not know a lot.	0.967
Privacy Awareness 1	Online companies seeking information should disclose the way the data are collected, processed, and used.	0.786
Privacy Awareness 2	A good consumer online privacy policy should have a clear and conspicuous disclosure.	0.872
Privacy Awareness 3	It is very important to me that I am aware and knowledgeable about how my personal information will be used.	1.124
Privacy Concern 1	It usually bothers me when online companies ask me for personal information.	1.008
Privacy Concern 2	It bothers me to give personal information to so many online companies.	0.909
Privacy Concern 3	Online companies may collect any information about me because I have nothing to hide	0.427
Privacy Concern 4	I am concerned that online companies are collecting too much personal information about me	0.844
Privacy Concern 5	I am not bothered by data collection, because my personal information is publicly available anyway.	0.873

4 HYPOTHESES

Our first hypothesis aims to explore the priming effects on user decision making when possible decisions are presented in a particular fashion. We expect participants who are not primed to consider all profiles and read through them while those who are primed are expected to skip liberal profiles faster. We state the hypothesis as follows:

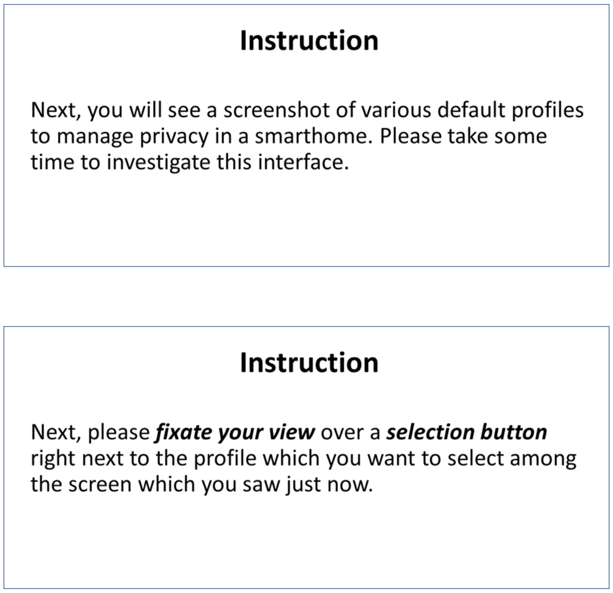
H1: Controlling for profile orders, priming has a significant effect on the eye fixations of participants.

Research has shown that there exists a gap between intention and behavior when people make decision [4]. There might be a similar gap in the IoT context as well and we intend to investigate it. Hence, our second hypothesis is as follows:

H2: The intent (fixations on Figure 1) is significantly different from the actual choice (fixations on Figure 2) which participants make when choosing a default setting.

It should be noted that in the above hypothesis, intention of the participant is measured as which of the profile, the participant fixates on most and behavior is the profile which the user will choose the second time when the same interface is shown with buttons. It is crucial to have the participants follow this exercise twice because in case of just having Figure 1 the participants will be just focusing on investigating the profiles however while in the decision page (Figure 2) the participants are forced to make a specific choice. This is where we expect to find our intention-behavior gap.

To summarize, this study will try to understand how users of IoT make the decision when they are primed with specific opinions about IoT. This study will also aim to investigate if there exists any intention-behavior gap in user decisions in context of IoT.



Instruction

Next, you will see a screenshot of various default profiles to manage privacy in a smarthome. Please take some time to investigate this interface.

Instruction

Next, please ***fixate your view*** over a ***selection button*** right next to the profile which you want to select among the screen which you saw just now.

Figure 3: From top a) First Instruction and b) Second Instruction

Table 3: T-Test results for various AOI's per image

AOI	Mean - Fixations/sec		p-value
	Positive	Negative	
EnableAll	6.32	7.90	0.056
DisableAll	5.98	7.99	0.234
No Sharing	7.15	7.53	0.648
Limited Tracking	6.42	7.46	0.421
Local Storage	8.62	8.23	0.852

5 RESULTS AND DATA ANALYSIS

5.1 Demographics

The study was conducted with 18 (Male: 11, Female:7) participants. The participants were recruited mainly from School of Computing at Clemson University Main Campus and majority (89.46%) of them being from Technical Background. Average age of participants was 23.5 years.

5.2 Differences in Priming Condition

We conducted analysis using R and R studio. Our study comprised of two groups, namely positive primed group and negative prime group based on the IoT introduction provided to them at the beginning of the study. Additionally, 5 AOIs per interface image were also present in our study for decision as well as observation stage of the study. To begin our analysis, we ran t-tests between positive and negative groups. We checked for differences in total viewing times and fixations per second across both the groups. The results from these tests are mentioned in Table 3.

Table 4: T-Test results for various AOI's per image

AOI	Mean - Total view time		p-value
	Positive	Negative	
EnableAll	4.45	2.99	0.189
DisableAll	1.35	1.19	0.799
No Sharing	7.15	7.53	0.648
Limited Tracking	4.96	5.38	0.809
Local Storage	3.78	3.74	0.973

5.3 Regression Models for Observation Image

To understand which profiles people looked at the most we also ran regression models. We used linear mixed effect model using 'nlme' package in R while also creating a random intercept to account for within subject variability. While this study is between subjects, the data was structured in a way that it needed to to treated as mixed effects. This is due to the fact that we had the timings, fixations and so on per participant per condition. We coded our regression models as follow:

fixations aoi+(1|participant)

We similarly ran the model by adding priming and the interaction effects between priming and aoi as well (See Table 5 and 6 for results).

Results show that the AOIs had a significant effect (Chi. Sq. = 32.24, p<0.001) on the total time viewed. Whereas priming did not have an effect (p = 0.809) on the same. It should be noted that the effect of AOI on total time as well as fixations (In Table 5 and 6) included the participant responses for both the priming together does not account for between subjects effects. To account for this, we also added the interaction effect of priming and AOI. However, we fail to see any such interaction effects.

5.4 Post Hoc Tests - Profiles which caught higher attention

During the analysis, we also ran several post-hoc tests for the effects of AOI on Time and Fixations. We split our data in two separate datasets, positive framing and negative framing.

We observed that compared to *Disable All* AOI, participants looked *Limited Tracking* AOI longer by 4.19 seconds (p<0.001) and *Local Storage* AOI longer by 2.7 seconds (p = 0.006). Interestingly, there was no significant difference (p = 0.163) between Disable All and Enable All AOIs. These observations are in case of participants who were given Negative Framing.

For the participants with Positive Framing, compared to *Disable All* AOI, participants looked at *Enable All* AOI longer by 3.10 seconds (p = 0.007) and *Limited Tracking* AOI longer by 3.61 seconds (p < 0.001). We did not observe any significant differences for other profiles. These observations are also visualized in Figure 4 and 5.

Based on the post-hoc analysis, it can be oberved that the participants on an average looked at *Limited Tracking* AOI higher than any other profile.

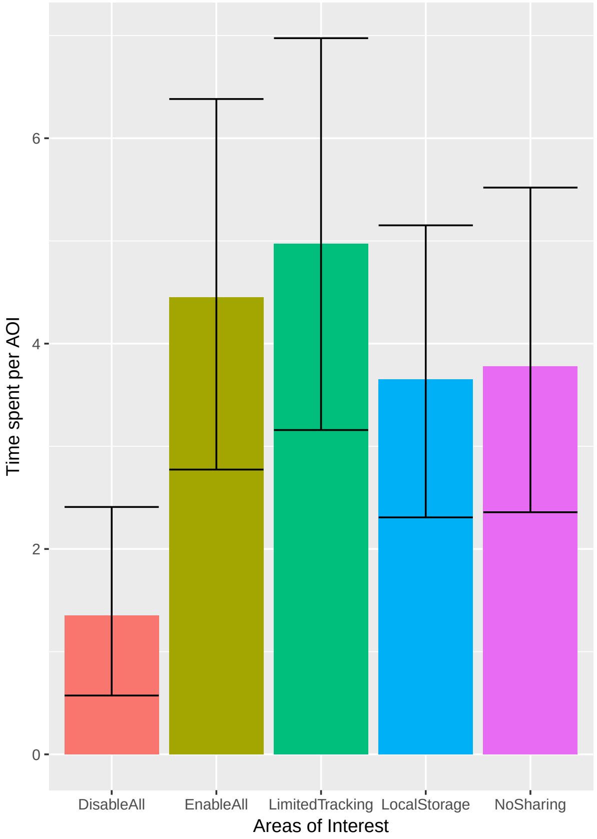


Figure 4: Plot for total time spent per AOI in Positive Priming

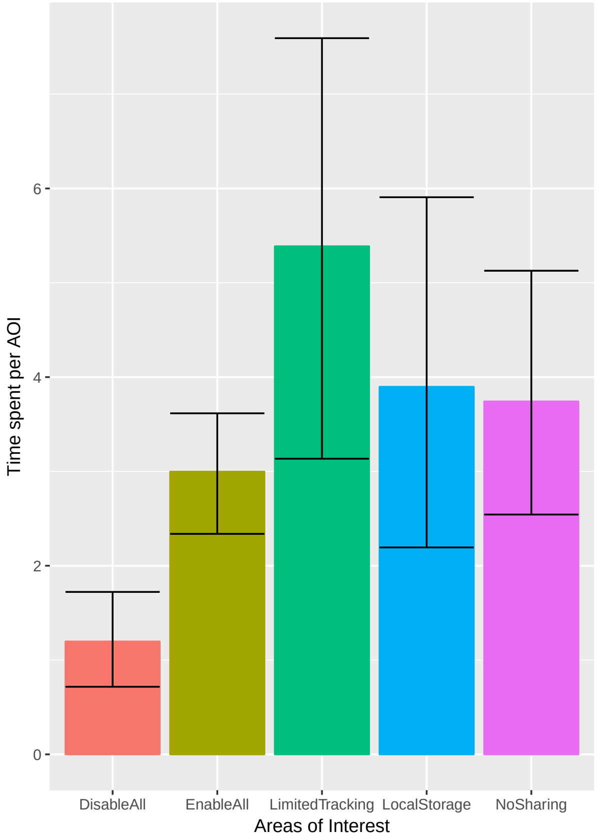


Figure 5: Plot for total time spent per AOI in Negative Priming

5.5 Post Hoc Tests - Profiles which were actually selected

For the Decision Image shown to participants who also received positive framing, we observed that compared to *Disable All* AOI, participants looked at *Enable All* longer by 5.49 seconds (p = 0.006). We did not observe any other significant differences across any other levels of AOIs.

Similarly, in case of decision image shown to participants who received negative framing, we observed that compared to *Disable All* AOI, participants looked at *Enable AOI* longer by 3.16 seconds (p = 0.026). We did not observe any other significant differences across any other levels of AOIs.

It should be noted that while we collected data from participants about their Knowledge, Privacy Concerns and Privacy Awareness using pre-validated scales, we did not include them in this data analysis. We conducted Confirmatory Factor Analysis of these scales and the model fit statistics were not satisfactory.

Table 5: Effect of AOI and Priming on Total Time

Model	χ^2	df	p-value
$time \sim (1\|sid)$			
+aoi	32.24	7	$< .0001$
+prime	0.05	8	.809
+aoi:prime	2.85	12	.581

Table 6: Effect of AOI and Priming on Saccades

Model	χ^2	df	p-value
$fixation/sec \sim (1\|sid)$			
+prime	3.05	7	.0807
+aoi	3.15	8	.531
+aoi:prime	1.16	12	...8

6 DISCUSSIONS

Our data shows that there are no significant priming effects on the time and fixations/second of the participants. However, the post hoc tests do show that the participants did pay attention to AOIs different across the different priming conditions. For example, in case of positive framing, there was a significant difference between how long participants looked at Enable All as opposed to Disable All. We did not see any such trend in case of Negative priming condition. Even the T-Tests are indicative of similar inference. Although not highly significant, the average amount of time spent on

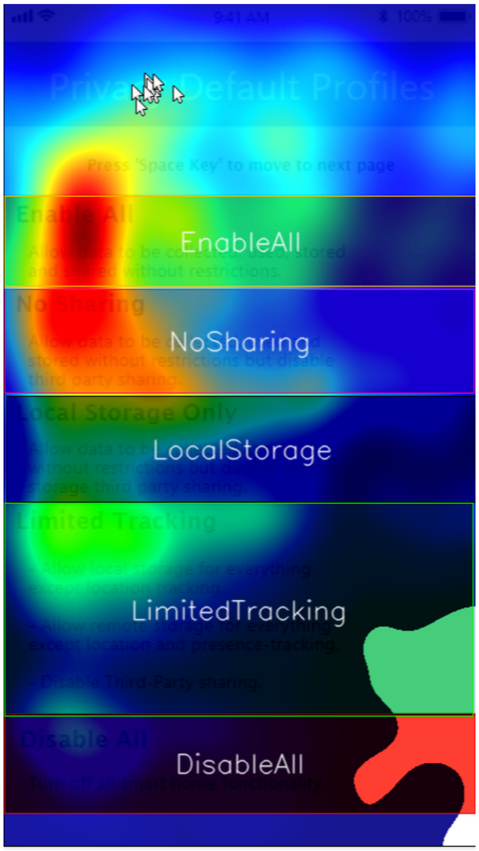


Figure 6: Heat Map for all the participants in the Positive Priming Condition

Enable all AOI for Positive Priming is 4.45 seconds as opposed to 2.99 seconds in Negative Framing condition (See Table 4. A closer observation of heatmap is also indicative that the participants in Positive conditions on an average spent more time looking at *EnableAll* AOI (See Figure 6. Both of these observations do indicate that priming certainly had the effect on which participants looked at the most. Based on the existing dataset, we can say that overall we do not have enough evidence to support H1.

The post hoc tests also indicate that the participants looked at *Limited Tracking* AOI longer that *Disable All* we believe that it does not have to do with the way priming had much effect on the participant observations. This can very easily be possible due to the larger size of this AOI and we are of opinion that this should be treated as a possible confound to our study.

Interestingly, the profiles which our participants focused more on in Decision Image had much striking difference with respect to Observation Image. For example, in case of Decision Image, for positive as well as negative priming, the only significant difference is that between *Enable All* and *Disable All* AOIs. Whereas, in case of Observation Image, for positive as well as negative framing, we observe significant differences across much more of the AOI including *Limited Tracking* and *Local Storage*. This indicates that participants when making decisions, tend to make much more polar choices. That is, they tend to make choices which are at the extremes, Enable or Disable.

Another interesting observation in this study is that there are no significant differences in *No Sharing* and *Limited Tracking* AOIs. This is strange mainly because the description of these profiles allow for key difference, which is whether their collected data gets shared or not. A result like this indicates potentially, people may want to make their decisions at the point of data collection rather than making changes post this collection happens.

7 CONCLUSION AND LIMITATIONS

The authors believe that the results of this study are interesting in the sense that they give insights about how priming affects the way people observe and make decisions about selection of privacy profiles for their Smart Home systems. Additionally, this study also points towards intention behavior gap based on the observation that the user focused longer on Enable and Disable All AOIs in Decision Image as opposed to Observation Image. This is only indicative of potential of finding this gap but not necessarily supporting the hypothesis for the same. This can be attributed to one of the limitations of this study, we tasked our participants to look longer at the profiles which they wanted to select in the decision page, thereby rendering us with data in terms of time of observations and fixations. This in fact is more of a binary decision and should be treated as such. In replicating this study with more number of participants, we would make the participants actually choose the profile perhaps by using a web based UI and get the data of actual selection.

Another key limitation to our study is the weak size and a far less diverse pool of participants which could potentially be the cause of high errors of our results. Most of our participant pool is comprised of students mainly from technical background, another problem being low age of the participant. Hence this dataset is not necessarily representative of the diverse population which potentially uses or will use Smarthome systems.

Acquisti et al. [1] showed that when information disclosure requests are made in an increasing order of sensitivity and intrusiveness, people tend to disclose less information. Future study could potentially also aim at understanding this phenomenon for our interfaces. For example, this could be achieved by changing the order in which the profiles are shown. Right now, we have Enable All at the top, which can be moved to the bottom and shown to participants as well.

The authors are however optimistic about the results and are of opinion that this study should be replicated by fixing the issues of existing setup to get much better results.

REFERENCES

[1] Alessandro Acquisti, Leslie K John, and George Loewenstein. 2012. The impact of relative standards on the propensity to disclose. *Journal of Marketing Research* 49, 2 (2012), 160–174.

[2] Dan Ariely. 2008. Predictably irrational: The hidden forces that shape our decisions. (2008).

[3] Paritosh Bahirat, Qizhang Sun, and Bart P Knijnenburg. 2018. Scenario context v/s framing and defaults in managing privacy in household IoT. In *Proceedings of the 23rd International Conference on Intelligent User Interfaces Companion*. ACM, 63.

[4] Michal J Carrington, Benjamin A Neville, and Gregory J Whitwell. 2014. Lost in translation: Exploring the ethical consumer intention–behavior gap. *Journal of*

Business Research 67, 1 (2014), 2759–2767.

[5] Mary J. Culnan. 1993. "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *MIS Quarterly* 17, 3 (1993), 341–363. https://doi.org/10.2307/249775 ArticleType: research-article / Full publication date: Sep., 1993 / Copyright Âĺ 1993 Management Information Systems Research Center, University of Minnesota.

[6] Leslie K. John, Alessandro Acquisti, and George Loewenstein. 2011. Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information. *Journal of consumer research* 37, 5 (Feb. 2011), 858–873. https://doi.org/10.1086/656423 ArticleType: research-article / Full publication date: February 2011 / Copyright Âĺ 2011 Journal of Consumer Research Inc.

[7] Daniel Kahneman and Amos Tversky. 1984. Choices, values, and frames. *American Psychologist* 39, 4 (1984), 341–350. https://doi.org/10.1037/0003-066X.39.4.341

[8] Robert S. Laufer and Maxine Wolfe. 1977. Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of social issues* 33, 3 (July 1977), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

[9] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15, 4 (Dec. 2004), 336–355. https://doi.org/10.1287/isre.1040.0032

[10] Amanda Nosko, Eileen Wood, Miranda Kenney, Karin Archer, Domenica De Pasquale, Seija Molema, and Lucia Zivcakova. 2012. Examining priming and gender as a means to reduce risk in a social networking context: Can stories change disclosure and privacy setting use when personal profiles are constructed? *Computers in Human Behavior* 28, 6 (2012), 2067–2074.

[11] PricewaterhouseCoopers. [n. d.]. Smart home, seamless life: Unlocking a culture of convenience. https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/smarthome.html

[12] Michael Schiessl, Sabrina Duda, Andreas Thölke, and Rico Fischer. 2003. Eye tracking and its application in usability and media research. *MMI-interaktiv Journal* 6 (2003), 41–50.

[13] Nili Steinfeld. 2016. âĂIJI agree to the terms and conditionsâĂİ:(How) do users read privacy policies online? An eye-tracking experiment. *Computers in human behavior* 55 (2016), 992–1000.