Scenario Context v/s Framing and Defaults in Managing Privacy in Household IoT

Paritosh Bahirat
Clemson University
Clemson, USA
pbahira@clemson.edu

Qizhang Sun
Eindhoven University of Technology
Eindhoven, Netherlands
q.sun.2@tue.nl

Bart P. Knijnenburg
Clemson University
Clemson, USA
bartk@clemson.edu

ABSTRACT
The Internet of Things provides household device users with an ability to connect and manage numerous devices over a common platform. However, the sheer number of possible privacy settings creates issues such as choice overload. This article outlines a data-driven approach to understand how users make privacy decisions in household IoT scenarios. We demonstrate that users are not just influenced by the specifics of the IoT scenario, but also by aspects immaterial to the decision, such as the default setting and its framing.

Author Keywords
Internet of Things; Privacy; Data-Driven Design.

ACM Classification Keywords
H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

INTRODUCTION
Users of household IoT devices have to make numerous privacy-related decisions. In this study, we look at two separate aspects of this decision-making environment (Figure 1). On the one hand, we provide participants with a scenario, which is a combination of carefully chosen parameters that objectively define the decision context. On the other hand, we manipulate the framing and default of the decision, which have been shown to heuristically influence users' decisions [1]. We intend to understand which of these two aspects dominate when users make their privacy decisions in a household IoT environment: are they driven more by the heuristics of how decision is framed, or do they make a more conscious decision based on their understanding of the scenario? The answer to this question has important implications for the design of intelligent privacy-setting interfaces.

EXPERIMENTAL STUDY
The data is obtained by surveying 1186 participants recruited through Amazon Mechanical Turk. Each participant was provided with 13 scenarios, which were a combination of different parameters ('Who', 'What', 'Purpose', 'Storage' and 'Action'), for example: "Your smart lighting system ('Who') uses a camera ('What') to detect your location in the house ('Purpose'). The data is stored locally ('Storage') and used to optimize the service ('Action'). Scenario assignment followed a mixed fractional factorial design, in which each participant received a different set of 13 scenarios, chosen from a pool of 4608 scenarios, which span all 4*12*8*4*3 possible combinations of parameters. After reading each scenario, participants were asked if they would enable or disable this scenario. The framing and default of this question was manipulated between-subjects at three levels each: positive framing ("Would you enable this feature?"), negative framing ("Would you disable this feature?") or neutral framing ("What would you do with this feature?"); combined with a positive default (enabled by default), negative default (disabled by default), or neutral default (forced choice).

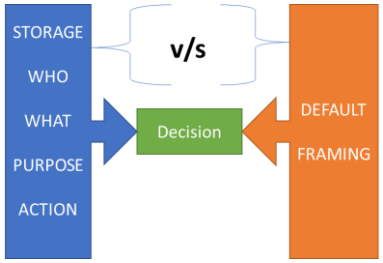

Figure 1. Parameters (blue) versus framing and defaults

DATA ANALYSIS
We split our data analysis into two parts. The first part is a *linear mixed effects regression* on the decision parameters. We iteratively add parameters to a base model, which has a random intercept for participants' repeated decisions. The Chi-square and p-values in Table 1 indicate the model improvement due to the addition of each variable. Notably, all parameters had a significant effect ($p < .05$) on participants' decisions. Figure 2 shows the percentage of participants' affirmative decisions for each level of the 'Storage' parameter. The graph shows that participants were significantly less likely to allow scenarios where data is shared to third parties, which is indicated by 'Sharing'. Our second *linear mixed effects regression* tests the effect of default and framing. Table 1 shows that both framing and default have a significant effect ($p < .05$) on participants' decisions. Figure 3 shows the percentage of participants'

IUI'18 Companion, March 7–11, 2018, Tokyo, Japan

ACM ISBN 978-1-4503-5571-1/18/03.
https://doi.org/10.1145/3180308.3180372

affirmative decisions for different defaults. In line with previous work on default effects [1], participants were less likely to allow scenarios when presented with a negative or neutral default, and more likely to allow scenarios when presented with a positive default.

Model	X^2	df	p-value
Decision~(1|userid)			
+storage	1505.461	2	<0.001
+who	189.185	7	<0.001
+action	76.845	3	<0.001
+purpose	205.965	3	<0.001
+what	213.079	11	<0.001
Model	**X^2**	**df**	**p-value**
Decision~(1|userid)			
+default	84.160	2	<0.001
+framing	6.2735	2	0.0432

Table 1. The effect of scenario context on decision, along with the effect of default and framing on decision.

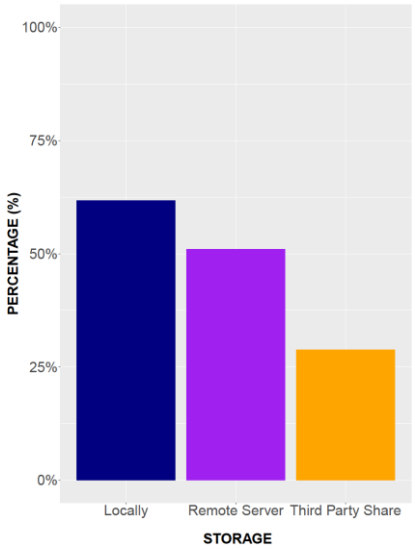

Figure 2. Percentage of participants deciding to 'enable' the feature for each level of the 'Storage' parameter.

CONCLUSION AND FUTURE WORK

The focus of our research is on understanding the privacy decision-making process of users in household IoT environments. We demonstrate that users' decisions are influenced by their careful evaluation of the scenario, as well as heuristic effects of the way the decision is presented to them. In future work we plan to analyze the cognitive processes that govern these two influences on users' decisions, and aim to find ways to minimize the heuristic influences of defaults and framing, e.g. by developing an interface that forces its users to conduct a conscious evaluation prior to enabling or disabling an appliance from collecting data. Moreover, we plan to use our findings regarding the scenario parameters to inform the development of interactive interfaces for household IoT environments. For example, understanding whether user perceives threats related to voice related data would help us gauge whether household IoT devices should use (or rather avoid) a voice-based interaction paradigm. Another example would be a *privacy-setting interface* that would prioritize parameters that have a strong effect on users' decisions. For example, based on our current findings, a household IoT privacy-setting interface should most prominently present privacy decisions regarding the storage of data, while decisions regarding the 'Action' can be relegated to "deeper" levels of the interface (cf. [2]).

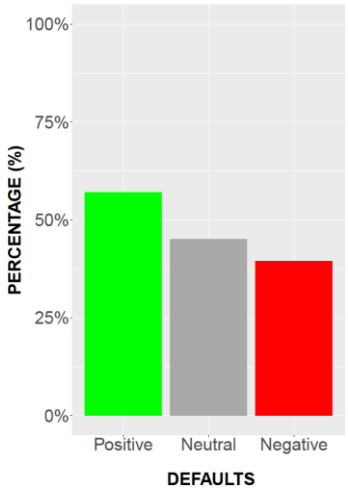

Figure 3. Percentage of participants deciding to 'enable' the feature for different default settings.

Finally, we plan to use default effects to our advantage, by tailoring the default settings in IoT privacy-setting interfaces to users' preferences regarding the various scenario parameters. As users tend to differ substantially in their privacy preferences, we envision such interfaces to contain a set of predefined "smart profiles" that cater to the preferences of a specific subset of users (cf. [2]). In conclusion, we believe that a data driven approach would be a good way to develop state of the art privacy management interfaces for household IoT platforms.

ACKNOWLEDGEMENT

This work was supported by NSF award no. 1640664.

REFERENCES

1. Eric J. Johnson, Steven Bellman, and Gerald L. Lohse. "Defaults, Framing and Privacy: Why Opting In ≠ Opting Out." *Marketing Letters* 13, no. 1 (2002): 5-15. http://dx.doi.org/10.1023/A:101504420

2. Paritosh Bahirat, Abhilash Menon, Yangyang He, and Bart P. Knijnenburg. "A Data Driven Approach to Developing IoT Privacy Settings Interfaces." In *Proceedings of the 2018 ACM International Conference on Intelligent User Interfaces* (IUI'18). http://dx.doi.org/10.1145/3172944.3172982