All in One! User Perceptions on Centralized IoT Privacy Settings

Karola Marky
TU Darmstadt, Germany
Keio University, Japan
marky@tk.tu-darmstadt.de

Kai Kunze
Keio University, Japan
kai@kmd.keio.ac.jp

Verena Zimmermann
Alina Stöver
Philipp Hoffmann
TU Darmstadt, Germany
zimmermann@psychologie.tu-darmstadt.de
stoever@psychologie.tu-darmstadt.de
ph.hoffmann@stud.tu-darmstadt.de

Max Mühlhäuser
TU Darmstadt, Germany
max@tk.tu-darmstadt.de

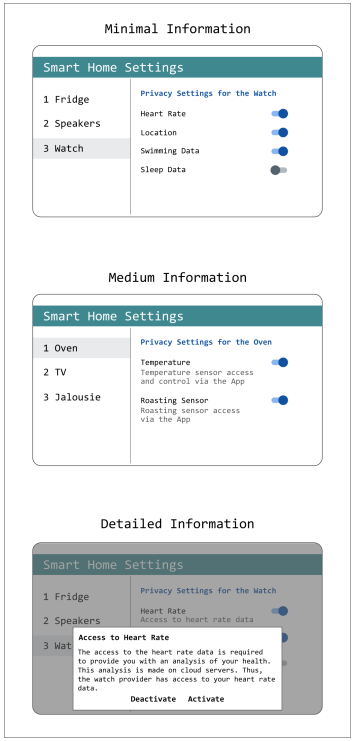

Figure 1: We investigate three different levels of information for adjusting privacy settings of IoT devices.

CHI '20 Extended Abstracts, April 25–30, 2020, Honolulu, HI, USA.

ACM ISBN 978-1-4503-6819-3/20/04.
http://dx.doi.org/10.1145/3334480.3383016

Abstract
IoT devices deliver their functionality by accessing data. Users decide which data they are willing to share via privacy settings interfaces that are typically on the device, or in the app controlling it. Thus, users have to interact with each device or app which is time-consuming and settings might be overlooked. In this paper, we provide a stepping stone into a multi-device interface for adjusting privacy settings. We present three levels of information detail: 1) sensor name 2), sensor name and information about captured data and 3) detailed information on each collected data type including consequences. Through a pre-study with 15 participants, we found that users prefer the access to detailed information because this offers the best decision support. They also wish for a clear status communication, a possibility for rule-based settings, and delegation options.

Author Keywords
Smart Home; Internet of Things; Privacy Decision Support

Introduction and Background
User settings are a collection of individual decisions that a user makes to determine how electronic devices should act. Privacy settings, in particular, reflect the user's decisions on how a device should collect, handle or share their data. They are widely used in, for instance, social networks [4, 10], online browsers [9], and IoT devices [2, 1].

The last mentioned IoT devices can deliver many benefits. Smart home devices, in particular, can improve home security, or the control over energy consumption (cf. [8]). But these benefits can only be delivered if the devices have access to data. The users of smart home devices accept sacrificing privacy for convenience [15, 5]. On the other hand, smart home devices should offer their users means to adjust the data collection to match their personal privacy needs [5, 12, 16]. Thus, users have to decide which data they are willing to share with each smart home device via privacy settings interfaces.

These interfaces are typically located either on the specific device, or in the app for controlling it. Therefore, users have to interact with each device or app which is 1) time-consuming, 2) settings might be overlooked, and 3) laymen might struggle in comprehending the settings.

To tackle these issues, we provide a stepping stone into a multi-device interface for adjusting privacy settings. In a pre-study with 15 participants, we investigated three distinct levels of information detail: 1) name of the sensor 2), and name of the sensor and information what this sensor does 3) detailed information on each collected data type including consequences. After interacting with each interface, we provided a questionnaire to collect preliminary feedback aiming to inform further studies. Our study shows that users prefer the ability to access detailed information on each sensor because this supports them best in making their decision. They furthermore wish for a clear status communication of the sensor, dynamic settings that are based on rules, and delegation options. Our pre-study aims to inform future studies of multi-device interfaces.

Settings Information Levels

The level of details of the presented information plays an important role in making a decision. For designing the multi-device interface for adjusting privacy settings, we commenced by investigating different levels of information to support the users in making privacy-related decisions. Hereby, we consider the following three levels of information detail: 1) minimal information, 2) medium information, and 3) detailed information. Details about each level are given below.

1) Minimal Information

In the minimal information level, we only provided the names of the sensors which are implemented in the device, e.g. "fridge content camera". Next to the sensor name, we placed a switch for controlling the sensor by switching it on or off Figure 2 shows a mockup of the minimal information level.

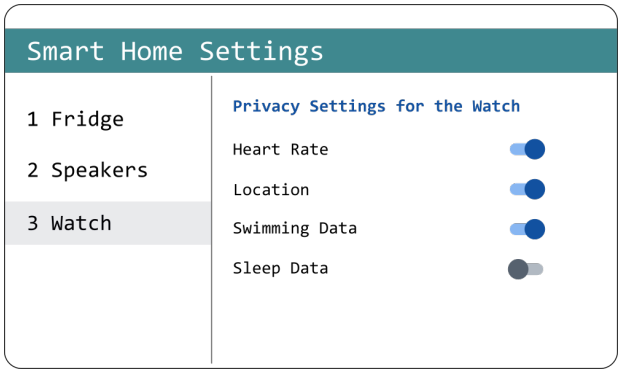

Figure 2: Mockup of the minimal information level

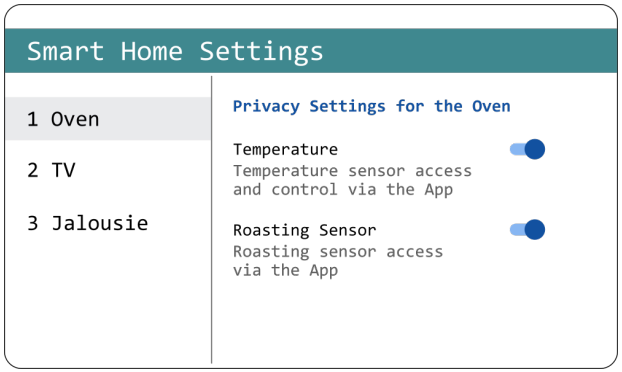

Figure 3: Mockup of the medium information level

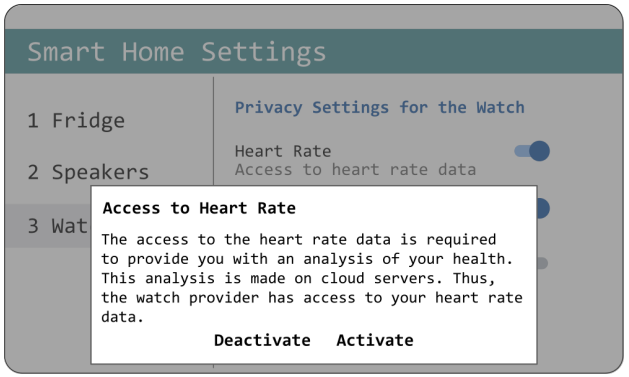

Figure 4: Mockup of the detailed information level

2) Medium Information
The medium information level extends the minimal level with a description of each sensor. This description provides information why this sensor is needed. For instance, "the fridge content camera is needed to show the fridge's content to you in the mobile app" (see Figure 3).

3) Detailed Information
The detailed information level provides a pop-up for each sensor. This pop-up contains detailed information why the sensors is needed, the consequences of its deactivation, as well as the parties who have access to the data collected by the sensor. For instance, "The fridge content camera is needed to show the fridge's content to you. The app that you use to access the camera picture has access to it. If you switch the camera off you can no longer see your fridge's content in the app" (see Figure 4).

We implemented a prototype interface for each of the three information levels as an Android app on tablet-PC. Each prototype provided settings for 24 IoT devices that are already available on the market. The devices were grouped into categories by the device type, such as smart health or smart household devices.

Method

To investigate user perceptions of the three settings interfaces and the detail of the provided information, we conducted a pre-study with 15 participants.

To be able to compare the different information levels with the same participants, we opted for a within-subjects design. The order of the conditions was given by a Latin square in order to avoid sequence effects. The procedure of our pre-study was as follows:

The participants were invited in our lab. We provided them with a consent form that included the study's data protection policy which is also compliant to the GDPR and national laws. After signing the consent form, the participant filled in a questionnaire which asked for demographics and previous experiences with the usage of smart home and IoT devices.

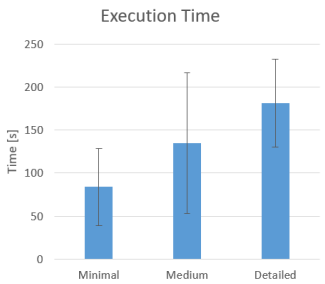

Figure 5: Bar chart of the execution time.

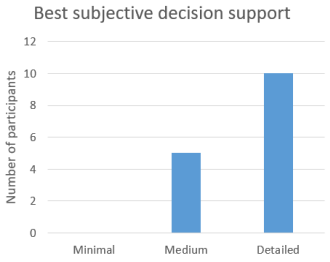

Figure 6: Bar chart of the preference shares regarding the best subjective decision support.

The participants were instructed to interact with the settings interfaces on a tablet. In particular, we asked them to adjust the settings of three devices for each condition according to their personal needs. The three devices were randomly assigned. After adjusting the settings, the participants could freely explore the app and interact with it.

When the participant reported completion of adjusting the settings and exploring, the examiner proceeded to the next condition. The interaction of the participant with the interface was recorded by a screen-capturing software.

After interacting with all three conditions, the participants received a questionnaire. In this questionnaire, we asked the participants for their favorite level of information. We also asked which interface supported them best to adjust the settings matching their privacy needs and were they would like to receive privacy-related information. The participants could also provide further general app-independent feedback and feedback for the three tested apps. Finally, the examiner thanked the participants and gave them the possibility to ask questions. We did not compensate the participants for participation.

Participants

Fifteen participants took part in our study. We recruited them via mailing-lists and forums. Three of them identified as female, eleven as male and one participant preferred not to answer. Their average age was 27.4 years ($SD = 13.3$, $Min = 18$, $Max = 57$). All participants either owned a tablet-PC or a smartphone, twelve were Android users and three used iOS. Furthermore, nine participants were active users of smart home or IoT devices.

Results

In this section, we report the results of our study.

Execution Time

We obtained the execution time from analyzing the screen-recordings of the interaction. As execution time, we consider adjusting the three assigned settings without the free exploration. Figure 5 depicts the execution time in the different information levels.

In the minimal information level, the participants needed on average 83.5 seconds ($SD = 45.1$, $Min = 25s$, $Max = 173s$), in the medium level, the needed 135 seconds ($SD = 82.0$, $Min = 44s$, $Max = 339s$), and in the detailed level they needed 181.7 seconds ($SD = 51.4$, $Min = 72s$, $Max = 242s$). We analyzed the execution with a Friedman test which reveals significant differences between the three conditions with $\chi^2(2) = 5.18$, $p = 0.012$.

To further investigate these differences, we ran Wilcoxon tests with a Bonferroni correction to account for multiple testing. The tests reveal significant differences between the minimal and the medium information level ($p = .04$), as well as between the minimal and the detailed information level ($p = .021$). Differences between the medium and detailed information levels could not be found ($p = 1.00$).

User Preferences

In the final questionnaire, we asked the participants which of the presented settings interfaces supported them best in making a decision that matches their privacy needs. Figure 6 depicts the shares of the different levels.

None of the participants stated that the minimal information would be sufficient for them. When asked to explain their answer, they named the missing explanations as a reason. E.g. P10 stated the following: *"This app did not offer any explanation."*[1]

[1] All comments were translated from German.

One third of participants ($N = 5$) said that the medium level of information was best for them to mark their decision. Sample comments from the participants are:

- *"App 1 offered too little information, App 3 offered too much information."*, P1
- *"The amount of information was clearest in this app, so I can well imagine reading and understanding all of it."*, P7

Two thirds of the participants ($N = 10$) felt that the detailed information level supported them best. Their comments are:

- *"The pop-ups with detailed information about the setting you want to change is very helpful. It gives precise information about the effects [...] Minimal prior knowledge is required. Experts do not need to read the text, for all others the text is helpful."* , P3
- *"This app provided the most contextual information, making a well-considered choice easy."*, P5

Besides the interface-specific questions, we also asked general ones about the information that the participants expected or wished to receive within a settings interface.

Thirteen of the fifteen participants wanted to receive information about the specific sensors and their purpose. When asked where they would expect such information, one participant stated that they wanted to receive it from the vendor's website, three participants would have liked to have it in the device's manual, and thirteen would have liked to get this information directly in the settings. Multiple answers were possible in this question. One participant did express the need for the access to any information. When asked to explain their answer that said *"as an expert, I already know this information."*

User Wishes and Suggestions
Finally, we asked the users how the interfaces could be further improved to better match their individual privacy needs. Here, we received three groups of answers: 1) the wish for security-related information (e.g., information on encryption), 2) the wish for rule-based settings (e.g., setting a time frame for data capturing) and 3) the wish for delegation options (e.g., delegating settings to an assisting software).

In the first group of answers, the participants stated, that the detailed information level should also contain information related to security. For instance, P12 said: *"Upon request, further technical background information, such as the method of transmission of the data, whether and which encryption methods are used and similar."*

The wish for rule-based settings considers that the presented interface only provided a static setting. The users either switch the sensor on or off. Settings could enable users to set rules when the sensors are on (time-based), or restrict the number of times that the sensor can capture data. For instance, the fridge's content camera could be switched off over night.

Finally, the wish for delegation refers to the possibility to let a trusted entity, such as a software or another person, such as an expert, adjust the settings for the user.

Discussion and Future Directions

We investigated a first prototype for a multi settings interface for adjusting the privacy settings of IoT devices. Such an interface could be part of a general control screen for such devices that is placed in the user's home.

Information Level and Placement
The majority of participants reported that the detailed information level supported them best in adjusting the settings

matching their privacy needs. This was despite the additional time they needed to make the settings. The participants valued the additional information and stated that it should be available even if it is not read by every user.

The vast majority of participants would expect to receive detailed information about the sensors, the data they capture and the recipients of the data in the settings. Therefore, privacy settings should offer such data. Future studies should also consider the changing needs for privacy-related information over time [6] and evaluate adaptable solutions.

Rule-Based Settings
Our participants expressed that static settings that offer switching on and off do not reflect all of their needs. Future studies should consider possibilities to set rules for settings. Instead, a setting is either on or off, it could be configured based on an underlying rule. Each a rule can be time-based meaning that users can set a time frame in which the sensor is allowed to capture data. Another rule could be limiting the number of times a sensor has access to data. For instance, the camera in a smart fridge could be accessed once per day. In doing so, it is less likely to capture people opening the fridge. Another example is limiting the Internet access of a device to several times per day if the information that is requests is not updated frequently.

Delegation
Participants can be overwhelmed with the number of decisions that they have to make. Furthermore, the decision might be too complex for them to handle. Participants in our study expressed the wish to delegate their privacy decision to a trusted person or even to a software assistant. Privacy assistants have already been investigated in smart homes [3] and related areas, such as smartphones [7].

Scalability and Other User Types
Since the amount of devices is likely to rise in the future, so will the amount of decisions to make. Thus, we consider the investigation of privacy assistants in the scope of IoT and smart homes to be an integral part of future work. A privacy assistant could be an AI that learns the decisions that the users make or another software that make decisions based on the users' privacy profiles [3]. Furthermore, up to now, we investigated the settings of primary users, smart home environments, however, can host other user types, such as visitors [14, 13, 11], who also might wish to exert control over the data collection.

Conclusion
In this paper, we report a preliminary investigation of user perceptions on different information levels with regards to a privacy settings interface. The results of the study show that users prefer the ability to access detailed information within the settings. Besides, our results indicate that static settings, meaning that the sensor is either on or off, is not enough to accurately reflect the users' needs. Thus, future studies should also consider rule-based settings that break the static nature of settings. Since this was a preliminary study, future studies should also investigate a more representative sample size.

Acknowledgement
This work has been co-funded by the German Federal Ministry of Education and Research (BMBF) within the SWC 2.0 "PrivacyGate" 01|S17050, by the Horst Görtz Foundation, by the BMBF and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE, and JST CREST Grant No. JPMJCR16E1 Experiential Supplements.

REFERENCES

[1] Paritosh Bahirat, Yangyang He, Abhilash Menon, and Bart Knijnenburg. 2018. A Data-Driven Approach to Developing IoT Privacy-Setting Interfaces. In *Proceedings of the International Conference on Intelligent User Interfaces (IUI '18)*. Association for Computing Machinery, New York, NY, USA, 165–176. DOI:http://dx.doi.org/10.1145/3172944.3172982

[2] J. Cornwell, I. Fette, G. Hsieh, M. Prabaker, J. Rao, K. Tang, K. Vaniea, L. Bauer, L. Cranor, J. Hong, B. McLaren, M. Reiter, and N. Sadeh. 2007. User-Controllable Security and Privacy for Pervasive Computing. In *Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications*. 14–19. DOI:http://dx.doi.org/10.1109/HotMobile.2007.9

[3] A. Das, M. Degeling, D. Smullen, and N. Sadeh. 2018. Personalized Privacy Assistants for the Internet of Things: Providing Users with Notice and Choice. *IEEE Pervasive Computing* 17, 3 (Jul 2018), 35–46. DOI: http://dx.doi.org/10.1109/MPRV.2018.03367733

[4] Serge Egelman, Andrew Oates, and Shriram Krishnamurthi. 2011. Oops, I Did It Again: Mitigating Repeated Access Control Errors on Facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. Association for Computing Machinery, New York, NY, USA, 2295–2304. DOI: http://dx.doi.org/10.1145/1978942.1979280

[5] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, USA, 399–412.

[6] Timo Jakobi, Gunnar Stevens, Nico Castelli, Corinna Ogonowski, Florian Schaub, Nils Vindice, Dave Randall, Peter Tolmie, and Volker Wulf. 2018. Evolving Needs in IoT Control and Accountability: A Longitudinal Study on Smart Home Intelligibility. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 4 (2018), 171. DOI:http://dx.doi.org/10.1145/3287049

[7] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun Aerin Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. 2016. Follow my Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. 27–41.

[8] Davit Marikyan, Savvas Papagiannidis, and Eleftherios Alamanos. 2019. A Systematic Review of the Smart Home Literature: A User Perspective. *Technological Forecasting and Social Change* 138 (2019), 139–154.

[9] Lynette I. Millett, Batya Friedman, and Edward Felten. 2001. Cookies and Web Browser Design: Toward Realizing Informed Consent Online. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '01)*. ACM, New York, NY, USA, 46–52. DOI: http://dx.doi.org/10.1145/365024.365034

[10] Mainack Mondal, Günce Su Yilmaz, Noah Hirsch, Mohammad Taha Khan, Michael Tang, Christopher Tran, Chris Kanich, Blase Ur, and Elena Zheleva. 2019. Moving Beyond Set-It-And-Forget-It Privacy Settings on Social Media. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*. ACM, New York, NY, USA, 991–1008. DOI: http://dx.doi.org/10.1145/3319535.3354202

[11] Katrin Wolf, Karola Marky, and Markus Funk. 2018. We should start thinking about Privacy Implications of Sonic Input in Everyday Augmented Reality!. In *Mensch und Computer 2018 - Workshopband*. Gesellschaft für Informatik e.V., Bonn, 353–359. DOI: http://dx.doi.org/10.18420/muc2018-ws07-0466

[12] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, USA. DOI: http://dx.doi.org/10.1145/3290605.3300428

[13] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security & Privacy Concerns with Smart Homes. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, USA, 65–80.

[14] Eric Zeng and Franziska Roesner. 2019. Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study. In *Proceedings of the USENIX Security Symposium (USENIX Security '19)*. USENIX Association, Berkeley, CA, USA, 159–176.

[15] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 200. DOI:http://dx.doi.org/10.1145/3274469

[16] Verena Zimmermann, Paul Gerber, Karola Marky, Leon Böck, and Florian Kirchbuchner. 2019. Assessing Users' Privacy and Security Concerns of Smart Home Technologies. *i-com* 18, 3 (2019), 197–216.