# An In-Depth Analysis of Security and Privacy Concerns in Smart Home IoT Devices Through Expert User Interviews

Sascha Löbner[1][0000−0001−9164−1919], Frédéric Tronnier[1][0000−0002−6202−4871], László Miller[1][0009−0000−0107−1052], and Jens Lindemann[2][0000−0003−0103−2461]

[1] Goethe University Frankfurt am Main, Germany sascha.loebner@m-chair.de
[2] Universität Hamburg, Germany jens.lindemann@uni-hamburg.de

**Abstract.** The integration of smart home IoT devices into households promises to improve users' living experiences and increase convenience, but raises manifold privacy and security concerns. This study conducts 11 interviews with expert users in Germany, employing qualitative content analysis to unveil prevalent privacy and security concerns. The objective is to survey smart home usage behavior and user knowledge to identify the need for solutions that educate users on potential threats, and aid them in securing their smart home. The findings illuminate the evolving dynamics of user perspectives within the rapidly advancing smart home landscape of IoT devices and the need for open-source solutions that provide recommendations and data flow control in smart home devices. Although knowledgeable in general, it can be observed that even expert users lack awareness of information flows in smart homes, calling for more education and the creation of software and hardware-based solutions to mitigate threats in the future.

**Keywords:** Smart Home · IoT · Security Concerns · Privacy Concerns · Privacy Awareness · Threat Mitigation · Usage Behavior

## 1 Introduction

The Internet of Things (IoT) promises to revolutionize modern living, envisioning a future where interconnected home devices communicate seamlessly to provide users with innovative and comfortable services.

Smart home devices, connected to the internet, and ideally each other, are supposed to automate tasks and workflows, thereby supporting users in their everyday life. Such devices include smart vacuum cleaners, home assistants, cameras, TVs, lights, temperature sensors and a variety of other solutions surrounding a persons' home. However, with a decrease in cost, an increase in capabilities, and a myriad of smart device providers, concerns arise with regard to the privacy and security of such devices. The ultimate aim of our research is to provide a solution that educates users on potential privacy and security issues in their smart home environment, and enables them to detect and prevent the undesirable transfer of data and information.

The final publication is available at Springer via https://doi.org/10.1007/978-3-031-62918-1_7.

As a first step towards this objective, this article aims to obtain feedback on the usage of smart home devices, understand potential privacy and security concerns, and explore existing or desired mitigation mechanisms. To achieve this, we follow a qualitative approach by conducting 11 semi-structured interviews with expert users that are analyzed using qualitative content analysis [12].

The results indicate that, although privacy and security concerns are prevalent, users cannot be easily clustered into groups, based on behavior or demographic properties. We find that more education on smart home usage, with regard to privacy and security threats, is necessary, and oftentimes desired by users. Moreover, interviewees express strong interest in future hard- and software solutions and outline several valuable ideas for features of such products.

## 2 Related Literature on Privacy in Smart Home Systems

Previous research has looked into different aspects of smart home users' concerns and shed light on how people view the way data is managed in their smart home envioronments. This section provides an overview of relevant studies that have looked into concerns about privacy connected to IoT devices.

Similar to our approach, Zheng et al. [21] utilize a qualitative approach and show that users' feelings about data collection are guided by the perceived benefits. For their 11 interviewed users from 8 households they find that users prioritize convenience and connectedness over privacy and security. While they only investigate the willingness to increase privacy and security, our survey goes one step further and investigates potential mitigation strategies that are already in use or desired by smart home device users with high IT knowledge. In their literature review on smart home users, Marikyan et al. [11] discuss benefits, device functionalities and barriers to smart home device adoption.

Lau et al. [9] conducted qualitative interviews and a diary study to investigate the adoption or non-adoption of smart speakers. They find that non-usage is caused by a lack of perceived utility and distrust in the producers of the speakers. Users are found to trade privacy for convenience and have a limited understanding of privacy risks. The authors furthermore find that privacy settings in smart speakers are rarely used, as they are not well aligned with users' needs. For instance, users asked for an incognito mode option for smart speakers, similar to web browsers, as well as for the option to prohibit the smart speaker from listening for a specific time frame, via voice commands.

Meng et al. [13] study intelligent personal assistant usage by conducting interviews with cohabitants and visitors of shared households. The authors find that both groups demonstrate similar concerns and attitudes with regard to data usage and monitoring. Furthermore, they perceive a lack of transparency. A perceived powerlessness and imbalance of control ultimately lead to many respondents resigning to accept perceived concerns when using smart assistants. Meng et al. [13] and Lau et al. [9] furthermore provide interview guidelines that have been adapted for this work. Apthorpe et al. [1] study privacy concerns among smart home device users, using contextual integrity (CI) theory by Nissenbaum

[15]. The authors conduct an experiment to observe differences in acceptability of flows of information for several smart home devices. Following CI, different recipients of information, different devices as senders of information as well as different information types are transferred under different information principles. They find that some transmission principles significantly increase or decrease acceptance of flow of information. Similarly, some smart home devices are viewed as more acceptable (e. g. power meters) than others (e. g. smart fridges).

Psychoula et al. [16] carried out a study to grasp the privacy worries among users of IoT devices. Their study revealed that participants had notable concerns about privacy when using IoT devices. Interestingly, younger users were more attuned to privacy matters compared to older generations. However, they also found that even though younger participants were concerned, they did not have specific knowledge about the types of data these devices collect.

In a similar study, Tabassum et al. [18] delved into user uncertainty regarding data practices with IoT devices. The researchers introduced a unique drawing task to bring out how participants conceptualize data flows between smart home devices and other entities. Surprisingly, participants' prior familiarity with smart home technologies did not really affect their actions to protect privacy. Instead, their concerns were mainly shaped by their experiences with other computer-related situations and organizations. Participants expressed a wish for more openness and control over how their data is gathered. Naeini et al. [14] conducted a thorough study with over 1,000 participants to examine the factors that influence privacy worries in IoT contexts. The study identified several factors that affect the level of privacy concern, including the kind of data gathered, third party sharing, and where data is collected. Participants also stressed how crucial it is to be informed about the collected data and how long it is stored.

Overall, the collected studies highlight common concerns among users of smart home devices. They also make clear that users want more information and authority over their IoT environment. Although the primary focus has been on participants from the US, it is crucial to realize that awareness and worries about data privacy and security can differ significantly between countries. For instance, Germans tend to be more aware of their privacy rights [7] and are more cautious about the gathering and use of their personal data compared to UK and US citizens [8]. These findings suggest that the outcomes of previous studies might not fully capture the privacy worries of the German population. This study adds to the existing research by addressing this gap and particularly concentrating on German individuals to scrutinize their current worries and setups regarding data privacy and security. Additionally, it recommends potential remedies and mitigation strategies to these concerns.

## 3 Methodology

As the objective of this document is to uncover the wishes and needs of users with regard to protecting themselves from undesirable consequences of the use of smart home devices, semi-structured interviews are conducted with experts on

the topic mainly. Respondents not only discussed the topic at hand through the eyes of an expert, but were also questioned on their own usage of, and attitudes towards, smart home devices. Semi-structured interviews allow more leeway to interact with the interviewee to assure that one captures all the nuances of a topic. Strictly following a structured interview might pose the risk of not being able to capture certain motives, for instance with regard to privacy concerns that interviewees might have, as no deviations from the pre-defined interview structure are allowed. The interviews were conducted in person or virtually using BigBlueButton, an open source video conferencing software. Interviews were recorded with the interviewees' consent and then automatically transcribed using Python and Whisper AI by OpenAI. The transcriptions were routinely compared with the original recordings by the interviewers. Transcriptions were then analyzed using MAXQDA, following the qualitative content analysis coding procedure by Mayring and Fenzl [12]. After the analysis, the recordings were deleted.

### 3.1 Participants and Data Processing

In total, 11 participants were interviewed. Six of these participants were recruited through German public Reddit forums to obtain participants who are not directly or indirectly related to the researchers and to ensure a wide variety of demographics. This voluntary participation ensured personal interest in the usage of smart home applications. The remaining participants were obtained through personal and work-related channels of the researchers, for example, through prior research collaborations and LinkedIn contacts. To satisfy ethical requirements, all participants participated voluntarily, and participants' consent was obtained for the recording and processing of all interview data for academic purposes. The recordings were transcribed and then deleted to limit the storing of personal data to a minimum. Transcriptions were further pseudonymized by omitting names, age, and other information that could aid in identifying participants, such as company names or exact dates. One test interview was conducted in order to refine the interview guidelines. As this test interview provided significant insights and caused only minor changes in the interview guidelines, it was included in the overall sample. We set the requirement to conduct interviews specifically with individuals who have expert knowledge on the topic of IoT and smart home devices through professional or work-related experience, as well as a high degree of personal interest in the topic. After all, the objective is to obtain feedback on current smart home usage by such experts. Respondents were thus chosen based on their professional experience by the researchers, and then asked to further self-assess their knowledge on the subject, before the start of the main interview. A respondent without such knowledge (participant no.6) was included for comparability. All interviews were conducted in German with German participants. Thus, the results are only of limited applicability to other contexts in terms of culture and country, while previous research, as discussed in Section 2, already focused on other countries and demographics.

### 3.2 Interview Guideline

Semi-structured interviews were conducted using a carefully designed interview guideline. Our guideline aims to strike a balance between allowing interviewees to freely express their opinions while also giving the interviews a clear structure to gather information relevant to the research questions. Important when creating the interview guideline was to avoid biases in responses, e.g., when participants say what they believe the interviewer would like them to say. This is known as confirmative response behavior or socially desirable responding [20].

Analogous to the privacy paradox observed in privacy research, wherein individuals' professed expectations regarding privacy frequently diverge from their actual behavior [5], the interview guideline consequently adopted an oblique approach to addressing concerns related to privacy. Instead of asking about privacy directly, the first sets of questions (A-H) surveys the actual usage of respondents' smart home devices. Only later on, privacy and security concerns are raised directly. Moreover, the interview was introduced as a general interview on smart home devices, without a specific reference to privacy or security concerns. The first sections of the interview guideline follow the questions by Meng el al. [13] and Lau et al. [9], who surveyed the usage of smart speakers and smart home assistants through qualitative approaches. Our interview guideline can be found in Appendix A and is structured in the following sets:

**Set A** discusses respondents' demographics such as age, profession and self-perceived level of IT knowledge.
**Set B** discusses the general internet provider setup of the respondent, as well as who is responsible for maintaining internet and device connectivity within the household.
**Set C** surveys smart home device usage and purchasing decisions. We also ask for reasons why certain devices are not used.
**Set D** collects general concerns about IoT device usage.
**Set E** delves deeper into the topic and discusses potential privacy concerns and discusses their effect on technology usage.
**Set F** discusses potential security concerns and their effect on technology usage.
**Set G** discusses the influence of controls on the IoT device setup.
**Set H** is about user story elicitation for improving the smart home environment with regard to privacy and security. Possible mitigation measures that respondents could or have taken to overcome said concerns are collected. Based on this, future research will aim to design products that match the users' needs as best as possible.

## 4 Results

### 4.1 Demographics

Table 1 depicts the demographics of participants. The average age of participants was 34 years. Of the 11 respondents, six lived in apartments, while the rest

**Table 1.** Demographics of interview participants

| Participant | Age | IT knowledge | Devices (D-ID) | Profession |
|---|---|---|---|---|
| 1 | 18-24 | 6.00 | 4 | Consultant |
| 2 | 18-24 | 8.50 | 2,5 | Student: Communica. Informatics |
| 3 | 25-35 | 7.50 | 1,2,5 | Computer Scientist |
| 4 | 36-45 | 9.00 | 1,6,7,8 | Computer Scientist |
| 5 | 25-35 | 7.00 | 6,7,8 | Student: Electrical Engineering |
| 6 | 36-45 | 8.00 | 5,7 | Private Investigator |
| 7 | 25-35 | 8.00 | 2,5,6 | Sales Representative |
| 8 | 36-45 | 7.50 | 1-3, 5-8 | IT Security Manager |
| 9 | 25-35 | 8.50 | 1 | Academic Research Assistant |
| 10 | 46+ | 9.00 | 2,3,8 | Electrician |
| 11 | 25-35 | 8.50 | 2,4,5 | Software Engineer |

lived in houses. A correlation between the number of devices and the living location could not be found. This is surprising, as we hypothesized that older people own or live in larger houses and thus have more smart home device applications. Again, we aimed for participants with high IT knowledge because we want to learn from them how they deal with security and privacy issues in smart homes and which countermeasures they use. The IT knowledge is based on a self assessment. Participants were asked how they would rate their knowledge on IT, computers and IoT devices, on a scale from 1-10 where 1 translates to "no knowledge" and 10 "expert knowledge". The average self-assessed IT knowledge was high at 7.95. Furthermore, the majority of respondents possess a professional background in computer science or IT.

### 4.2 Smart Home Setup

All participants were able to explain how they set up their system. Nine out of 11 have set up the system by themselves. Three participants stated that they had created a closed system for smart home devices, meaning a specifically created IoT hub to enhance data control and processing. One of the participants lived in shared accommodation, which introduces unique privacy and security scenarios since trust scenarios might differ from traditional households. All users confirmed that they were using a router and had access to it. This confirms basic IT knowledge about network setup for smart home devices among all participants.

### 4.3 IoT Device Usage

Table 2 depicts the device types present in respondents' households. Participants own on average 2.9 smart home devices. The main motivation for smart home device usage is to increase convenience and quality of life (n=6). The devices used most often are smart lights and smart assistants such as Amazon's Alexa. It is

**Table 2.** Smart device information

| D-ID | Type | Count | Example |
|---|---|---|---|
| 1 | Robo vacuum cleaner | 4 | iRobot |
| 2 | Smart assistant | 6 | Amazon Alexa |
| 3 | Smart camera | 2 | Ring |
| 4 | Smart TV | 5 | Samsung TV |
| 5 | Smart light | 6 | Philips Hue |
| 6 | Smart temperature/air | 4 | Humidity sensors |
| 7 | Other sensors | 4 | Door sensors |
| 8 | Other devices | 4 | Garden watering |

important to take into account that some devices, such as smart garden watering, can only be used by house owners with gardens. According to Statista [19] 71 % of German households own a smart TV. One reason for the lower number in our survey might be the fact that smart TVs can be substituted by other devices, e. g. laptops, which may be likely especially for students. Respondents might also not be aware that they indeed own a smart TV, especially if they do not specifically use its smart functionalities.

### 4.4 Identified Constructs and Factors

The main focus of this survey is the investigation of possible solutions to improve smart home security. Thus, we ordered the question sets D - G by identified constructs or factors influencing smart home device adaption. We first investigate privacy and security concerns, followed by currently implemented and potential future mitigation strategies to protect smart home IoT environments.

**Privacy Concerns:** The majority of participants stated the importance of privacy in general as well as for smart home devices (n=9). The dichotomy between privacy and usability or convenience was immediately brought up by two participants, while three participants mentioned a need for retaining control over data. Four participants stated that privacy had been a substantial factor for the decision not to purchase certain smart home devices. Privacy concerns were raised through news stories or movies, according to three participants.

**Security Concerns:** They appear to be less present than privacy concerns. One stated reason for this observation is that participants specifically decided for smart home devices which they perceived as being secure. Three participants justified their purchase decisions despite security concerns with their personal assessment of the trade-off between security concerns and gained usability.

One participant reported that specialized media outlets warned about a specific software bug for smart home locks: *"And there was a power failure, and that somehow led to the hardware that was installed assuming that this was now a dangerous situation. And then his front door was open." (Participant 7)* According to the respondent, who uses these locks, the issue has not been fixed by the producer. At the time of the interview, the respondent was still using the smart

lock, since he concluded based on his personal assessment that the situation is acceptable. Such concerns were shared and discussed with friends and family.

**Data Storage:** There was significant uncertainty regarding the storage of data gathered by smart home devices. Five participants stated that data was sent to and stored on manufacturers' servers, which might also be outside the European Union. Respondents were not sure how long the data was stored, six participants assumed that it might be stored permanently. According to the GDPR, personal data must not be stored longer than necessary for the intended processing of the data. The deletion of personal data by manufacturers was highly questioned by respondents. For example, Participant 7 reported:

*"[...] in my old job, I changed jobs four months ago, there were also situations where users could delete things, but they weren't deleted at all, they were just no longer displayed as visible and I just assume Amazon and all the big companies, I have to say, actually, that things are never really deleted, but are just always hidden, because they need these data for whatever analysis, evaluation, training, they are kept." (Participant 7)*

Even data security experts acknowledged that they did not inform themselves exactly in which country device manufacturers process and store data, although these respondents had expressed concerns about data protection and security earlier in the interview. Thus, more transparent information similar to model cards [2], adapted for individual IoT devices, could be helpful.

**Data Sharing and Processing:** Respondents believe that product manufacturers utilize the data for their own purposes. Three respondents stated that third parties are also able to process the data, while one respondent believed that IT personnel of a manufacturer would technically be able to access the data, but would not make use of this due to the data solely being analyzed and processed automatically. There exist reports that such smart home device data has been accessed in the past by manufacturer personnel, for instance for smart home cameras or Tesla vehicles [17]. Respondents expressed the hope for limited sharing and that the processing would only be for the improvement of services that benefit users. However, all participants stated that they likely agreed to all data sharing, storing and processing by accepting the manufacturers' terms and conditions. This acceptance is also based on the concern that refusal would lead to a (partial) loss of functionality (n=3).

**Mitigation Measures:** As observed in existing research [9, 13], respondents felt that their options to cope with privacy and security concerns, or to mitigate potential risks, are limited. Ultimately, respondents largely accept the risks, after analyzing the trade-off between convenience and concerns (n=5), even though they stated that they could do more to protect their data. While two participants were not interested in more control over their data, the majority of participants stated that device manufacturers did not do enough to protect personal data. One participant differentiated between solutions provided by the product manufacturer and measures that the user can take. One solution that could be offered by the manufacturer was stated to be the offering of privacy and security settings. In this case a user could actively decide to enable or dis-

able specific settings, such as the sharing of data to improve services. Mitigation measures implemented or known by users are the following:

1. The use of DNS blockers and distributed networks (VLANs and guest/subnetworks) to separate different smart devices from each other. Alternatively, users could even use an individual Wi-Fi network for each smart home device.
2. Users could analyze or monitor data packets and traffic themselves, although this measure was deemed too technical for the smart home context.
3. Users could use firewalls to prohibit devices from communicating externally, which could hinder usability of the device.

One participant mentioned that he uses the open-source solution "Home Assistant" [6] to control smart home devices and retain privacy. This solution encompasses some of the desired features for future smart home privacy-enabling solutions. The same participant mentioned a friend that only bought hardware solutions that were deemed secure by him, without any cloud computing capabilities. However, the technical knowledge required for these solutions was deemed very high and not applicable for most users.

**Trust:** Trust was identified as a major factor supporting smart home device usage. In general, European Regulation, in the form of the GDPR, is seen as a substantial source of trust, even though participants lacked concrete information on data processing, sharing and storage. European companies are seen as generally more trustworthy than Chinese manufactures (named explicitly).

Regarding the size of companies, there were different opinions. On the one hand, large and established players are found to be more trustworthy than small companies and startups, due to perceived unstructured processes and the uncertain future of small companies. Although large tech organizations, such as Apple, Amazon or Alphabet, are known by respondents for their large-scale data processing, they are still seen as the "lesser evil". One explanation is again that their solutions are already in use by participants, both in their personal home and in the work environment. It was reported that a decision to trust or not trust has to be made and that it is easier to make this decision once for a big player compared to several small ones. This aligns with Zheng et al. [21], who find in their interviews a high influence of brand reputation on trust. On the other hand, an argument for choosing small companies is their better specialisation in their activities. The location of the company headquarters within a trustworthy country and potential funding from public bodies were also mentioned to increase trust.

## 5 Discussion

### 5.1 Recommendations for Implementation

In this section we collect recommendations for the design of future hardware and software solutions, based on the results identified in the previous chapter, with the aim to improve privacy and security in smart homes.

**Open-source:** Six participants suggested the solution to be open-source. This would foster trust in the manufacturer and the working mechanisms of the solution, e. g. due to community reviews and improvements.

**Community support:** Five participants stated that a community would provide a useful feature for them. This could include sharing of useful settings, warnings and suggestions for or against products and solutions as well as community-created databases. However, such involvement contradicts with the participants who stated that the majority of "normal" users would like to not think about the topic at all, and prefer to continue to do so in future.

**Outbound traffic analysis:** Four participants stated that analyzing all data flows of all smart home devices would be useful. This would provide a benefit in the form of a holistic overview of devices in smart home networks and inform users about device behavior. However, one respondent stated that any actions based on data flow analysis should only be taken by the user.

**Usability:** Two participants highlighted that a user-friendly design is a prerequirement for the implementation of any such hard- or software solution.

**Device recommendations:** One participant suggested a traffic light system to indicate secure, potentially dangerous and dangerous devices.

**No limitation of functionality:** Respondents stated that any software or hardware product should not limit the existing and used functionalities of smart home devices in any way. This is in line with the foundational principle "full functionality" of privacy by design [4].

**Education:** To satisfy the users' explicit desire to acquire knowledge in data privacy and security, solutions should strive to provide educational resources [21].

### 5.2 Impact

This study provides insights into challenges and concerns with regard to privacy in smart homes. With our results we aim to provide a solid base for improved regulation of smart home devices, striving to create policies that balance technological innovation with consumer security and privacy. The insights generated through the interview process reveal that even experts and avid users of smart home devices are uncertain about the nature of data processing, ranging from the specific data that is transferred, to transmission principles and potential data recipients. While there exist mitigation strategies, these are found to be complex and challenging for layman users. In future work, our insight will provide the basis for the development and design of hardware and software products that align usability and users' needs for security and privacy, especially on the German and European market. Moreover, this work underscores the importance of educating IoT users about potential threats and equipping them with the knowledge and tools to navigate these risks effectively, thereby enhancing their ability to make informed decisions about their smart home device usage. Guidance and motivation to implement education in IoT, privacy and security solutions is a key outcome of this research.

### 5.3 Limitations

The results of this work may be limited in generalizability as only German-speaking respondents with expert knowledge on IoT and smart home devices were considered. Existing research demonstrates that in particular privacy concerns and preferences differ, already on an EU-level [7, 8]. To increase accessibility, interview guideline and results are therefore translated into English. Moreover, participant selection was limited to people with high self-assessed expert knowledge, which could only be assessed indirectly through the analysis of responses afterwards. Furthermore, preferences of expert users might not represent those of average users. Thus, as a next step, large-scale quantitative surveys should be conducted to validate the findings of this work.

### 5.4 Future Work

This work is the starting point for user story elicitation and use case design. Based on our results we plan to design, implement and evaluate soft- and hardware solutions to educate smart home users on potential privacy and security risks, with the overall aim to enable users to control the processing of personal data. Along with these studies we plan additional quantitative surveys to evaluate usability, achieved privacy, security, trust and the education level with regard to IoT threats and solutions. Next steps are user story elicitation and use case design to close the market gap of smart home privacy and security soft- and hardware solutions, with a special focus on usability for average users. This especially holds for the integration of AI into IoT smart home devices [10].

## 6 Conclusion

With the constantly growing interconnectivity and data transfer between IoT devices, there remains a notable lack in user-friendly solutions to mitigate privacy and security threats and concerns in smart home ecosystems. Possible mitigation methods, such as separated WiFi networks or VLANs, are not intuitive to layman users, exhibit low usability, and are even to tiresome for expert users. In this qualitative work, we conducted 11 interviews with expert users to elicit a collection of possible measures and factors that need to be included in future solutions that aim to secure data flows in smart home ecosystems and educate users about actions they can take to increase the security of their smart home environment. Based on expert responses, user-friendly functionalities include open access services, device recommendations and ensuring full functionality while being able to control data flows within and between smart home devices. In the future, our goal is to develop hardware and software solutions, complemented by comprehensive usability studies, to ensure the full functionality of existing smart home environments while protecting privacy.

**Acknowledgments.** The project FIIPS-at-Home was funded by the German Federal Ministry of Education and Research under the funding code 16KISA068K. Responsibility for the contents lies with the authors. The project was funded by the European union – NextGeneration EU. The views expressed are those of the authors and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the European Commission can be held responsible for them.

**Disclosure of Interests.** The authors have no competing interests to declare that are relevant to the content of this article.

## References

1. Apthorpe, N., Shvartzshnaider, Y., Mathur, A., Reisman, D., Feamster, N.: Discovering smart home Internet of Things privacy norms using contextual integrity. Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies **2**(2) (2018)
2. Bracamonte, V., Pape, S., Löbner, S., Tronnier, F.: Effectiveness and information quality perception of an AI model card: A study among non-experts. In: 2023 20th Annual International Conference on Privacy, Security and Trust (PST), IEEE (2023)
3. Bracamonte, V., Pape, S., Loebner, S.: "All apps do this": Comparing privacy concerns towards privacy tools and non-privacy tools for social media content. Proceedings on Privacy Enhancing Technologies **3**, 57–78 (2022)
4. Cavoukian, A.: Privacy by design (2009)
5. Gerber, N., Gerber, P., Volkamer, M.: Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Computers & Security **77**, 226–261 (2018)
6. Home Assistant: Home assistant – open source home automation (2024), URL https://www.home-assistant.io, accessed: 2024-01-10
7. Ilhan, A., Fietkiewicz, K.J.: Data privacy-related behavior and concerns of activity tracking technology users from Germany and the USA. Aslib Journal of Information Management **73**(2), 180–200 (2021)
8. Kozyreva, A., Lorenz-Spreen, P., Hertwig, R., Lewandowsky, S., Herzog, S.M.: Public attitudes towards algorithmic personalization and use of personal data online: Evidence from Germany, Great Britain, and the United States. Humanities and Social Sciences Communications **8**(1) (2021)
9. Lau, J., Zimmerman, B., Schaub, F.: "Alexa, stop recording": Mismatches between smart speaker privacy controls and user needs. In: Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018) (2018)
10. Löbner, S., Pape, S., Bracamonte, V.: User acceptance criteria for privacy preserving machine learning techniques. In: Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES) (2023)
11. Marikyan, D., Papagiannidis, S., Alamanos, E.: A systematic review of the smart home literature: A user perspective. Technological Forecasting and Social Change **138**, 139–154 (2019)
12. Mayring, P., Fenzl, T.: Qualitative inhaltsanalyse. Springer (2019)

13. Meng, N., Keküllüoğlu, D., Vaniea, K.: Owning and sharing: Privacy perceptions of smart speaker users. Proceedings of the ACM on Human-Computer Interaction **5**(CSCW1) (2021)
14. Naeini, P.E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L.F., Sadeh, N.: Privacy expectations and preferences in an IoT world. In: Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), pp. 399–412 (2017)
15. Nissenbaum, H.: Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press (2020)
16. Psychoula, I., Singh, D., Chen, L., Chen, F., Holzinger, A., Ning, H.: Users' privacy concerns in IoT based applications. In: 2018 IEEE SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI, pp. 1887–1894, IEEE (2018)
17. Reuters: Tesla workers shared sensitive images recorded by customer cars. Reuters (April 2023), URL https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/
18. Tabassum, M., Kosinski, T., Lipford, H.R.: "I don't own the data": End user perceptions of smart home device data practices and risks. In: Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019), pp. 435–450 (2019)
19. Tenzer, F.: Anteil der TV-Haushalte in Deutschland mit Smart TV. https://de.statista.com/statistik/daten/studie/325527/umfrage/anteil-der-tv-haushalte-in-deutschland-mit-smart-tv/ (2023), accessed: 2024-01-10
20. Wetzel, E., Böhnke, J.R., Brown, A.: Response Biases. In: The ITC International Handbook of Testing and Assessment, pp. 349–363, Oxford University Press (2016)
21. Zheng, S., Apthorpe, N., Chetty, M., Feamster, N.: User perceptions of smart home IoT privacy. Proceedings of the ACM on Human-Computer Interaction **2**(CSCW) (2018)

# A Appendix – Interview Guideline

To create our semi-structured interview guideline, we consulted relevant literature [3, 9, 13] and translated the English version into German for the interviews.

**Question Set A: Demographics and basic questions**

1. Kindly introduce yourself. How old are you, what is your profession, where and how do you live?
2. What is your profession/degree?
3. How would you rate your knowledge on IT, computers and IoT devices on a scale 1-10 where 1 translates to "no knowledge" and 10 to "expert knowledge"?

**Question Set B: Internet and Home Set Up**

1. Can you explain to us how you set up your current internet connection?
2. Are you using a router?
3. Who was responsible to set up the working internet connection?
4. Who is managing it or conducting maintenance on it?

**Question Set C: IoT Usage**

1. Can you think of any smart home device that you are currently using? E.g. smart speakers/locks/curtains/heating/gardening systems, smart appliances (fridge, microwave, ...), light bulbs, Amazon Alexa, Apple HomePod.
   - Via app, via speech or in some other way?
   - For what purposes? Examples include alarm clocks, weather information or switching devices on and off.
   - How frequently?
   - Are there other people in your home that have access to or use the devices?
2. Why do you use the devices?
3. If you do not use any devices, why not?
4. Can you tell us how you first heard about such devices?
5. What did you think about them? What factors did you consider in your decision to buy/not buy such devices?
6. Did other people factor into your decision making process (For example: children, roommates, significant other)? Does their usage differ from yours?
7. Have you read or seen any additional information that influenced your decision making process? Such as reviews, technical articles etc.?

**Question Set D: General Concerns**

1. Do you have any concerns when using your WiFi or IoT devices?
2. Have there been any instances when you forgot that a device was on? Tell us about a recent time that this has happened.
3. Have there been any instances where you felt uncomfortable around the device? Tell us about a recent time that this happened.
4. Did you do anything to address your discomfort? What did you do? How satisfied are you with [workaround] in addressing your discomfort?

**Question Set E: Privacy Concerns**

1. What does privacy mean to you?
2. How does privacy fit into your life?
3. Can you tell us about specific instances or concerns about privacy that you've experienced with any technologies?
4. Do you have privacy concerns in general when it comes to technology, or is it specific to the Internet and IoT devices?
5. Can you tell us what led you to being concerned for your privacy?
6. How do these concerns affect how you use technology, if at all?
7. Did you have any concerns with how the [IoT devices currently used or discussed so far in the interview] would handle your privacy?

**Question Set F: Security Concerns**

1. What does security mean to you in this context?
2. Can you tell us about specific instances or concerns about security that you've experienced with any technologies?
3. Do you have security concerns in general when it comes to technology, or is it specific to the Internet and IoT devices?
4. How do these concerns affect how you use technology, if at all?
5. Did you have any security concerns with IoT devices?

**Question Set G: Controls**

1. When you were doing research on IoT devices and setting up your home internet, did security and privacy controls factor into your decision? (Controls as in to control privacy, security settings and related factors?)
2. Would you consider these security and privacy controls sufficient?

**Question Set H: User Stories**

1. Are you currently using any devices, Apps or software solutions such as firewalls to improve the security of your network or your smart home devices?
2. Are you aware of any specific security or privacy threats that might impact you, your home network or your devices?
3. What potential negative consequences could there be for you?
4. Regarding the transfer of data, such as information, text, video or sound recordings: Who would you not like to receive this kind of information? (E.g. device manufacturers, friends and family, BigTech, governments, governmental authorities, other unknown parties)
5. What information or devices would you like to protect the most? Are there devices and information that are more important than others?
6. What kind of solution would you prefer? An app or a physical device connected to your home network?