Home Sweet Home? Investigating Users' Awareness of Smart Home Privacy Threats

Nina Gerber, Benjamin Reinheimer, Melanie Volkamer
SECUSO (Security, Usability, Society)
Karlsruhe Institute of Technology
Kaiserstrasse 89
76133 Karlsruhe
{nina.gerber,benjamin.reinheimer,melanie.volkamer}@kit.edu

ABSTRACT

Albeit providing many benefits, smart homes collect and process large amounts of sensitive data. In order to successfully cope with the resulting risks for their privacy, users have to be aware of potential privacy threats and consequences in the first place. Since research in other contexts has shown that users often lack this awareness even when it comes to well-known technologies, e.g., Online Social Networks (OSN), it is crucial to investigate users' awareness of threats related to the use of unfamiliar technologies like smart homes. To this end, we conducted a survey study with 1052 lay users. By prompting participants to state all consequences that could potentially result from using smart home and smart health devices as well as OSN, we find that most participants were unable to state a single privacy consequence. Instead, most referred to general privacy issues (e.g., profiling, data collection) or threats related to non-privacy topics, such as security problems resulting from defect smart home devices. Since our participants were least aware of potential privacy consequences resulting from the use of smart home devices, further effort is necessary to inform lay users about possible privacy threats, e.g., by launching public campaigns or conducting trainings and interventions directly implemented in the UIs of smart home systems.

1. INTRODUCTION

It has been suggested that the main reason for lay users not to protect their private data, e.g., by configurating their privacy settings when using Online Social networks (OSN), is lacking awareness of possible consequences that could arise from data sharing [4]. Hence, if users are also unaware of potential consequences arising from the collection and processing of their private data in smart homes, they will not be motivated to invest time in the configuration of these complex systems in order to protect their data.

We therefore conducted a survey study with 1052 participants to investigate lay users' awareness of adverse consequences that could result from data sharing in smart homes. We decided to split our sample by prompting participants to state all potential consequences that could result either from using smart home devices, smart health devices, or Online Social Networks (OSN), in order to interpret the results with respect to users' awareness of privacy consequences associated with the use of established (OSN) and other leading-edge technologies (smart health devices).

We used a closed coding approach for the analysis of our data, classifying the responses based on the seven categories of privacy consequences proposed by Karwatzki et al. [5]. We find that most participants were not able to name a single adverse consequence which could arise from sharing their data when using smart home and smart health devices, or OSN. Instead, most of the responses either refer to general privacy issues (e.g., profiling or privacy violation) without mentioning specific consequences which could result from these issues, or consequences which are not related to the disclosure of private data, but to other challenges of digital technologies, e.g., security threats resulting from defect smart home or smart health devices. Furthermore, our participants were least aware of privacy consequences resulting from the use of smart home devices. If smart home privacy consequences were stated, they mainly referred to the loss of resources (e.g., money and time) or freedom, e.g., due to manipulation of users' decisions regarding their grocery shopping.

2. METHODOLOGY

We conducted a survey study with open answer questions to investigate of which consequences that could result from using unknown and well-established privacy-threatening technologies lay users are aware of.

2.1 Recruitment and Participants

We recruited our participants using the German panel "clickworker" [3]. A total of 1113 participants completed our study. Of these, 61 had to be excluded from the analysis since they did not respond to the open-answer question asking about potential consequences. The final sample thus includes 1052 participants (466 female, 578 male, 3 others, 5 chose not to answer this question). Participants ages ranged from 18 to at least 76 years (see Table 1). Most participants reported to use OSN often or sometimes, whereas only about one third stated to use smart home or smart health devices frequently. Participants reported a median of 0 years of IT security expertise. According to the IUIPC questionnaire

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018.
August 12–14, 2018, Baltimore, MD, USA.

Table 1: Participants' age.

Age	< 20	$20 - 25$	$26 - 35$	$36 - 45$	$46 - 55$	$56 - 65$	$66 - 75$	$76 - 85$	> 85
N	55	209	351	206	135	76	17	1	0
%	5.2	19.9	33.4	19.6	12.8	7.2	1.6	0.1	0

[8], participants were rather concerned about their privacy with an average of 3.51 (the scale ranges from 1 to 5, with 1 indicating low levels of concern; SD=0.75; med=3.5). All participants received a compensation of 2,10€.

2.2 Use Cases

We investigate three different use cases of which one (OSN) is well-known to most users and two (smart home and smart health devices) are a rather new topic to the majority of lay users. This approach allows us to compare lay users' awareness of privacy consequences associated with smart home use to those related to already established and other emerging technologies.

We used the following definition of smart home and smart health devices for our study: A smart home is a household in which household appliances (e.g., refrigerator, washing machine, vacuum cleaner), integrated devices (e.g., lights, windows, heating) and entertainment electronics (e.g., TV, game consoles) are networked and can be controlled via the Internet. Smart health comprises health care devices (e.g., blood pressure monitors, scales, thermometers) and special sensors (e.g., drop-sensors, sensors in the toilet, heat sensors) which are connected to the Internet [1, 7].

2.3 Study Procedure

We used a between-subject design, randomly assigning participants to one of the three considered technologies. All questionnaires were presented in German and implemented in SoSciSurvey [6]. The study procedure is described in detail below.

Welcome and Informed Consent. We first thanked participants and provided them with information about our study (i.e., length, purpose, compensation, anonymity of their data, opportunity to withdraw from participation at any time). Participants were asked to provide their consent for participation and processing of their data by clicking on a button which was labeled with "I agree". We then asked participants to indicate whether they used the three considered technologies, and if not, whether they liked to use them in the future.

Introduction of Use Case. Participants were then randomly assigned to one specific technology which was introduced to them in a brief descriptive text. In case they do not use the assigned technology, participants were prompted to imagine they would actually use it.

Open Question on Privacy Consequences. We used an open answer format to ask participants about possible privacy consequences. They were provided with ten text boxes and instructed to enter one consequence per box, beginning with the most severe one: "Please enter all the consequences that may arise from [scenario]. Please begin with the most severe possible consequence and leave the additional boxes empty if you do not know any further consequences." They further had the opportunity to provide as many additional consequences as they wanted in an extra text box at the end of the site.

Privacy Concerns and Demographics. At the end of the study, participants completed the IUIPC questionnaire's global information privacy concern scale [8]. Finally, we asked them to indicate demographic information. On the last page, we thanked the participants and provided them with contact details in case any questions would occur, as well as the code they needed to receive their compensation from the panel.

2.4 Ethics

All relevant ethical preconditions given for research with personal data by our university's ethics committee[1] were met. On the start page, all participants were informed about the purpose and procedure of the present study. Participants had the option to withdraw at any point during the study without providing any reason and we informed them that in this case all data collected so far would be deleted. Participants were assured that their data would not be linked to their identity and that the responses would only be used for study purposes. Furthermore, we used SoSciSurvey [6] for the survey implementation, which stores all data in Germany and is thus subject to strict EU data protection law.

2.5 Data Analysis

We used a closed coding approach to categorize all responses referring to specific consequences based on the seven categories proposed by Karwatzki et al. [5]. Conducting 22 focus groups, Karwatzki et al. [5] derive seven categories of privacy consequences users are aware of: physical, social, resource-related, psychological, prosecution-related, career-related, and freedom-related consequences.

The coding was conducted independently by two researchers, resulting in a Cohen's Kappa of 0.996 for the smart home devices, 0.96 for the OSN, and 0.99 for the smart health devices use case.

3. RESULTS

We received a total of 2462 responses. Of these, however, only 262 described specific consequences resulting from data sharing. The frequency of these consequences with regard to the seven privacy categories proposed by Karwatzki et al. [5] is displayed in Table 2.3. Furthermore, an overview is provided in Figure 1. Of the remaining responses, 964 referred to general privacy issues without stating actual consequences, e.g., data collection, profiling, or privacy violation (see Figure 2). 1265 responses described either general issues or specific adverse consequences, which are not related to data sharing or privacy infringement, e.g., security threats due to technical defects of the smart home or smart health devices. Finally, 134 responses referred to positive aspects of smart home, OSN, and smart health device usage, such

[1]A link to our university's ethics committee will be included in the non-anonymized version of the paper.

Table 2: Frequency of consequences stated in the seven categories after Karwatzki et al. [5]

Use case	Physical	Social	Resource-related	Psycho-logical	Prosecution-related	Career-related	Freedom-related	Total
Smart home devices	0	1	19	7	0	0	20	47
OSN	17	95	3	0	3	28	7	153
Smart health devices	2	4	36	12	0	12	6	72
Total	19	100	58	19	3	40	33	262

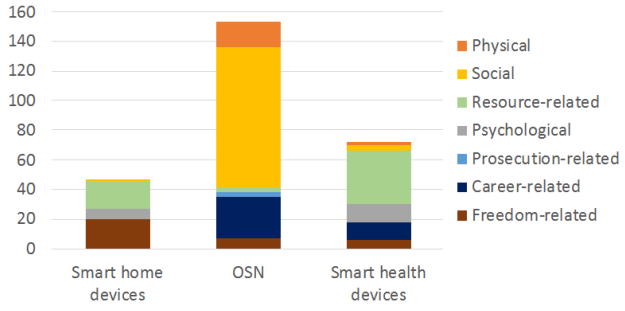

Figure 1: Frequency of consequences stated in the seven categories after Karwatzki et al.

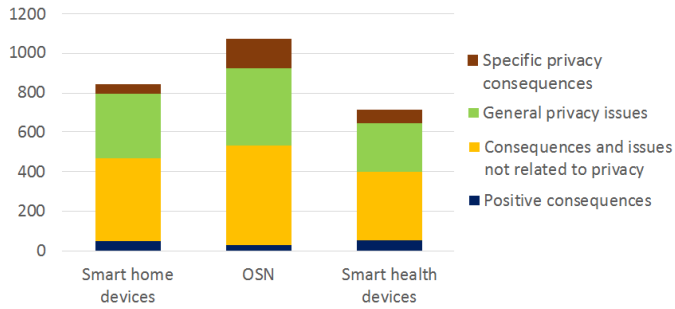

Figure 2: Frequency of responses describing specific consequences, general issues, adverse consequences and issues not related to privacy, and positive consequences.

as convenience or feeling connected to other people.

Only 47 specific privacy consequences were stated relating to the use of smart home devices, compared to 72 associated with the use of smart health devices and 153 for using OSN. Most of the stated privacy consequences relating to smart home use were freedom- or resource-related. No physical, prosecution-related or career-related consequences were stated.

Overall, the most specific consequences resulting from data sharing were provided in the OSN use case. Not surprisingly, the vast majority of these are attributed to the social category, followed by career-related and physical consequences. The most frequently stated privacy consequences resulting from the use of smart health devices are resource-related, followed by psychological and career-related consequences.

Over all use cases, social consequences were most frequently stated, followed by resource-related, career-related, and freedom-related consequences.

4. DISCUSSION

Asking 1052 participants to state consequences resulting from using smart home devices, OSN, and smart health devices, we find that most participants did not state a single specific consequence associated with data sharing. In fact, most of the responses described either consequences that were not related to the disclosure of private data, but, for example, to security threats resulting from defect smart home or smart health devices, or referred to privacy issues in general without mentioning specific consequences that could result from this issue (e.g., data collection, privacy violation). Specific privacy consequences were stated least frequently in the smart home use case. These results suggest that most lay users are indeed unaware of adverse consequences which could arise from using smart home devices, but also lack awareness of privacy threats related to the use of OSN and smart health devices.

Hence, it is necessary to inform users about such potential consequences. This could be done, for example, by launching public awareness campaigns, or developing trainings on this topic. Further approaches include interventions directly implemented in the respective applications and technologies, e.g., in the configuration interfaces of smart home systems.

Considering that most of the privacy consequences related to the use of OSN that were stated described social issues, users seem to lack the imagination of possible privacy consequences related to other domains. The outcries in social media following the Cambridge Analytica scandal [2, 9], including the "#deletefacebook"-campaign [10], indicate that these rather unknown privacy consequences might be better suited to motivate users to protect their privacy than these users are already aware of.

4.1 Limitations and Future Work

Several limitations apply to our study. First, since we only included participants who currently lived in Germany, our results may not be generalizable to other cultures. However, we are currently planning to conduct a follow-up study with participants from other European countries to allow for comparison of the results across a wider range of cultural backgrounds. Second, we used a panel to recruit our participants, thus it is likely that our sample is biased in terms of age, academic background and technical expertise, as it might be younger, higher educated and overly tech-savvy. Third, we only considered possible privacy consequences related to three use cases. It would be worthwhile to conduct another follow-up study to check whether the results also

apply to other use cases. Furthermore, it should be investigated if providing participants with a more comprehensive explanation of smart home and smart health devices leads to different results, since most of them may be rather unfamiliar with those technologies.

5. ACKNOWLEDGMENTS

This paper is supported by European Union's Horizon 2020 research and innovation programme under grant agreement No 740923, project GHOST (Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control). This work was also supported by the German Federal Ministry of Education and Research in the Competence Center for Applied Security Technology (KASTEL).

6. REFERENCES

[1] M. M. Baig and H. Gholamhosseini. Smart health monitoring systems: an overview of design and modeling. *Journal of medical systems*, 37(2):9898, 2013.

[2] C. Cadwalladr. 'i made steve bannon's psychological warfare tool': meet the data war whistleblower. https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump. Accessed: 2018-05-13.

[3] clickworker GmbH. clickworker panel, 2017. Accessed 2017-09-20.

[4] V. Garg, K. Benton, and L. J. Camp. The privacy paradox: A facebook case study. In *The 42nd Research Conference on Communication, Information and Internet Policy*, 2014.

[5] S. Karwatzki, M. Trenz, V. K. Tuunainen, and D. Veit. Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence. *European Journal of Information Systems*, pages 1–28, 2017.

[6] D. J. Leiner. Sosci survey (version 2.5.00-i), 2017. Accessed 2017-09-20.

[7] A. Lymberis. Smart wearable systems for personalised health management: current r&d and future challenges. In *Engineering in Medicine and Biology Society, 2003. Proceedings of the 25th Annual International Conference of the IEEE*, volume 4, pages 3716–3719. IEEE, 2003.

[8] N. K. Malhotra, S. S. Kim, and J. Agarwal. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, 15(4):336–355, 2004.

[9] M. Rosenberg, N. Confessore, and C. Cadwalladr. How trump consultants exploited the facebook data of millions. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. Accessed: 2018-05-13.

[10] H. Timms and J. Heimans. #deletefacebook is just the beginning. here's the movement we could see next. http://fortune.com/2018/04/16/delete-facebook-data-privacy-movement/. Accessed: 2018-05-23.

APPENDIX

Categories of Privacy Consequences Proposed by Karwatzki et al.

Physical: Loss of physical safety owing to access to individuals' information

Social: Change in social status owing to access to individuals' information

Resource-related: Loss of resources owing to access to individuals' information

Psychological: Negative impact on one's peace of mind owing to access to individuals' information

Prosecution-related: Legal actions taken against an individual owing to access to individuals' information

Career-related: Negative impacts on one's career owing to access to individuals' information

Freedom-related: Loss of freedom of opinion and behaviour owing to access to individuals' information