Identification and Influence of Perceived Risks on Smart Speaker Use Behavior

Maximilian Haug[1], Philipp Rössler[1], Heiko Gewald[1]

[1] Neu-Ulm University of Applied Sciences, Neu-Ulm, Germany; maximilian.haug@hs-neu-ulm.de, philipp.roessler@online.de, heiko.gewald@hs-neu-ulm.de

Abstract. Smart speakers gain more and more attraction from users. However, the technology is still relatively new and users feel uneasy about how and what functionality to use. This research investigates users' perception about risks associated with the use of smart speakers. In a qualitative study in which users could engage with smart speakers for a 2-month time frame, we found that risks show to be partly hypothetical and users develop unlikely risk scenarios which prevent them from using the whole functionality spectrum of a smart speaker.

Keywords: Smart Speaker, Perceived Risks, Privacy, Security.

1 Introduction

Jeff Bezos, science-fiction enthusiast and founder of Amazon, pushed the development of their first smart speaker Amazon Echo to grasp a bit of the future [1]. Since its release such as Alexa in 2014, smart speakers found their way into more and more homes and enjoy great popularity [2] and what previously used to be only in the movies is now reality.

Smart speakers are voice operated assistants designed to facilitate the everyday lives of their owners. To date there are several features available for smart speakers, such as playing music, purchasing products, control devices in smart homes, deliver information or create to-do lists. The interactions between user and smart speaker are voice-based and therefore the microphones of the devices are continuously listening for the wake-word (e.g. Alexa) [3].

Research on adoption behavior of voice operated devices is currently scarce. Furthermore, literature shows a wide variety of definitions for such devices. Intelligent voice assistants (IVA) [4, 5],voice-activated personal assistant (VAPA)[6, 7], voice-activated intelligent assistant [8], voice-activated assistant [3], intelligent personal (or personalized) assistant (IPA) [2, 9-11], virtual (or digital) personal assistant [2, 8], voice controlled (or conversational) agents [2] or ubiquitous personal assistant (UPA) [11] all refer to a voice operated device. This missing consensus on the terminology alone indicates that the field is relatively new and needs clarification. Little is known about the adoption behavior of smart speakers and in particular the risks associated with the use. Due to this relative new technology, people do not yet know what to expect from

15th International Conference on Wirtschaftsinformatik,
March 08-11, 2020, Potsdam, Germany

https://doi.org/10.30844/wi_2020_l5-haug

know what to expect from using it and associated risks may prevent them from using them in the first place. Therefore, we want to shed light on the questions:

RQ1: Which perceived risks are associated with the adoption and use of smart speakers?
RQ2: How do privacy concerns change over the time while using smart speakers?

To answer this research question 19 participants were recruited with the possibility for them to get access to a smart speaker and to use it for two months. In total 16 participants were interviewed before giving them the smart speaker and after the time frame of two months. Two of the participants did not want to use the smart speakers, while one participant already used them frequently. For the last three cases only one interview was conducted. The results show that risks associated with the technology are privacy, security and surveillance related. Over the time of the use, especially security risks emerged in the heads of the participants, which ultimately did not occur.

2 Literature Review

In the context of IoT devices, privacy concerns show to be a widely discussed topic. Due to the near impossibility to measure privacy itself, literature suggests that privacy concerns should act as a proxy [12]. Xu, Dinev [13] developed a model which suggests that privacy concerns emerge from individual characteristics or situational cues. Privacy experiences such as the exposition to former privacy issues are shown to influence privacy concerns (Smith). Furthermore, privacy awareness, which refers to how good individuals are informed about privacy issues, shows to trigger privacy concerns [14]. Personality and demographic differences, such as being an extrovert or an introvert, male or female also showed to influence privacy concerns [15-17].

Several studies suggest that privacy in the context of IoT is an issue, not least on the basis of the high possibility of security risks [18-20]. Eavesdropping, unauthorized access, data modification, data forgery and unauthorized remote tampering with devices are mentioned among the possibilities in how to abuse IoT devices [21, 22]. Therefore, unsecure data can leak to third parties in which case the control over the own data will be lost [21].

Another perspective on privacy is the privacy calculus, which assumes a tradeoff between risks and benefits which leads to a certain behavior [23, 24]. In the calculus privacy risk is defined as the individual belief of the potential loss of data which was disclosed to a firm [25]. Literature showed that privacy risk positively influences privacy concerns [26].

The literature on privacy showed that privacy concerns can be treated as a dependent variable [12], which is influenced by the individual differences as well as the environment individuals act in. Furthermore, the literature review suggests that

https://doi.org/10.30844/wi_2020_l5-haug

privacy and security in the case of IoT should not necessarily be viewed as independent concept, but rather be seen as how security affects privacy concerns.

3 Research Method

In the middle of 2019 in total 19 participants were recruited to take part in a qualitative data collection. The age of the participants ranged from 22 to 61 years and they showed different backgrounds in terms of IT affinity as well as prior experience with smart speakers. The participants were interviewed at the beginning of the study to understand their relation to smart speakers. Here, special emphasis lied on the risks associated with the technology. After the interview the participants, who did not already have a smart speaker (in this case Amazon Alexa was used as a smart speaker device) were asked to use one for the next 2 months. After this time frame the participants were interviewed again to understand whether their perception shifted. From the sample of 19 participants, 2 did not want to take part in the study (no smart speaker use and therefore no second interview). One participant already had experience using a smart speaker for 2.5 years. 16 participants did not initially have a smart speaker and were willing to take part in the study. From the last group of the sample there is an interview before and after the 2-month period. Three out of the 19 participants were female. Almost all participants had some kind of interaction with a voice operated device such as Siri or Cortana. The interviews were recorded and transcribed. Two researcher independently used open coding for the interviews and triangulated the data following the recommendation of Huberman, Miles [27] and Flick [28]. The interviews were coded based on topics which were identified in literature, such as privacy risk, security risk and surveillance anxiety. After 19 participants we observed a saturation of the information provided by the participants so that no additional information was to be expected from further interviews.

4 Results and Discussion

The relationship between user and privacy is a rather ambivalent one. The participants for a majority do not know how the abuse of their data might manifest in a malicious way. The users of smart speakers show concerns since they feel to have no control on their personal information, which might be collected and used by the manufacturers. In this way the participants feel interfered in their privacy. Due to this, two participants (P5 and P19) didn't want to participate in the experiment, but others mentioned their concerns towards privacy as well (as indicated by the citations above). The interviews also show a different facet of data disclosure. They indicate a certain lack of power concerning their data:

P2_1: Thus, your data is disclosed, and it doesn't matter, because everybody knows your data already.

https://doi.org/10.30844/wi_2020_l5-haug

In terms of privacy the study showed that the participants had concerns from the beginning in contrast to the security risks. This indicates that privacy plays a bigger role in the initial adoption of the technology than security risks. In line with Wirth, Maier [33] we found a rather ambivalent relationship of users with the privacy topic as indicated in the results. Even though there seems to be a big awareness of privacy issues associated with the technology, there is also a certain resignation present. Users feel like they do not have control over their data anyways. This is in line with the findings of Wirth, Maier [33] who found that privacy risks in the context of social networking sites do not have a significant influence on the intention to self-disclose.

The results showed that over time, users develop concerns towards the security aspects with smart speakers. This concern is linked with the increasing possibilities which users associate with the technology. The mentioned risks however are also present in technology which is used already today. Credit card theft e.g. can also happen while using the standard webpage of Amazon, still people usually do not see a problem doing their online shopping there. Therefore, for practical implications, manufacturers of smart speakers should sensitize their users by addressing common risks associated with the technology. This way, users get more comfortable with smart speakers and the associated risks may not play as big of a role. In the current situation smart speakers are simply too new for people to grasp the whole concept and possibilities, which leaves a lot of space for creativity what could go wrong, which in turn prevents them from using it. Furthermore, the manufacturers can also gain a better reputation if they can communicate transparently what and how data is used in the process.

5 Limitations and Further Research

This research has several limitations. First of all, due to the qualitative approach in the study, we cannot make strong claims about the strengths of influences on adoption or continuous use behavior. It is also possible that the participants answer in a way that is viewed favorable by others, which is called social desirability response [34]. With a sample of 19 the generalizability is limited, however the interviews gave deep insights into the individual's perception. Furthermore, the study is based on a convenience sample from south Germany. However, we tried to keep the sample as mixed as possible in terms of age and prior experience, to grasp the whole spectrum of associated risk.

Researchers should investigate specific use-cases of smart speakers to reduce the complexity of the acceptance. The possible categorization into inbuilt functionalities, e-commerce and controlling other devices were already pointed out and in addition, use-cases can be created.

References

[1] Steinharter, H. and T. Kuhn, *Künstliche Intelligenz - Bitte ein Bot*, in *Wirtschaftswoche*. 2016. p. 51-52.

[2] Lopatovska, I., et al., *Talk to me: Exploring user interactions with the Amazon Alexa.* Journal of Librarianship, 2018.

[3] Crossler, R.E., K.-K.R. Choo, and F. Bélanger. *Intelligent Home Assistant Use in the Home Environment*. in *Twenty-fourth Americas Conference on Information Systems*. 2018. New Orleans.

[4] Appiah Otoo, B. and A.F. Salam, *Mediating Effect of Intelligent Voice Assistant (IVA), User Experience and Effective Use on Service Quality and Service Satisfaction and Loyalty*, in *Thirty ninth International Conference on Information Systems*. 2018: San Francisco.

[5] Hoy, M.B., *Alexa, Siri, Cortana, and More: An Introduction to Voice Assistants.* Med Ref Serv Q, 2018. **37**(1): p. 81-88.

[6] Moorthy, A.E. and K.-P.L. Vu, *Privacy Concerns for Use of Voice Activated Personal Assistant in the Public Space.* International Journal of Human-Computer Interaction, 2014. **31**(4): p. 307-335.

[7] Mallat, N., V. Tuunainen, and K. Wittkowski. *Voice Activated Personal Assistants - Consumer Use Contexts and Usage Behavior*. in *Twenty-third Americas Conference on Information Systems*. 2017. Boston.

[8] Jiang, J., et al., *Automatic Online Evaluation of Intelligent Assistants*, in *Proceedings of the 24th International Conference on World Wide Web - WWW '15*. 2015. p. 506-516.

[9] Han, S. and H. Yang, *Understanding adoption of intelligent personal assistants - A parasocial relationship perspective.* Industrial Management & Data Systems, 2017. **118**(3).

[10] Goksel-Canbek, N. and M.E. Mutlu, *On the track of Artificial Intelligence: Learning with Intelligent Personal Assistants.* International Journal of Human Sciences, 2016. **13**(1).

[11] Mihale-Wilson, C., J. Zibuschka, and O. Hinz, *About user preferences and willingness to pay for a secure and privacy protective ubiquitous personal assistant*, in *Twenty-Fifth European Conference on Information Systems (ECIS)*. 2017: Guimarães.

[12] Smith, H.J., T. Dinev, and H. Xu, *Information privacy research: an interdisciplinary review.* MIS quarterly, 2011. **35**(4): p. 989-1016.

[13] Xu, H., et al., *Examining the formation of individual's privacy concerns: Toward an integrative view.* ICIS 2008 proceedings, 2008: p. 6.

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

[15] Xu, H., *The effects of self-construal and perceived control on privacy concerns.* ICIS 2007 proceedings, 2007: p. 125.

https://doi.org/10.30844/wi_2020_l5-haug

[16] Bansal, G. and D. Gefen, *The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online.* Decision support systems, 2010. **49**(2): p. 138-150.

[17] Chen, K. and A.I. Rea Jr, *Protecting personal information online: A survey of user privacy concerns and control techniques.* Journal of Computer Information Systems, 2004. **44**(4): p. 85-92.

[18] Airehrour, D., J. Gutierrez, and S.K. Ray, *Secure routing for internet of things: A survey.* Journal of Network and Computer Applications, 2016. **66**: p. 198-213.

[19] Fink, G.A., et al. *Security and privacy grand challenges for the Internet of Things*. in *2015 International Conference on Collaboration Technologies and Systems (CTS)*. 2015. IEEE.

[20] Henze, M., et al., *A comprehensive approach to privacy in the cloud-based Internet of Things.* Future Generation Computer Systems, 2016. **56**: p. 701-718.

[21] Malina, L., et al., *On perspective of security and privacy-preserving solutions in the internet of things.* Computer Networks, 2016. **102**: p. 83-95.

[22] Porras, J., et al. *Security In The Internet Of Things-A Systematic Mapping Study*. in *Proceedings of the 51st Hawaii International Conference on System Sciences*. 2018.

[23] Klopfer, P.H. and D.I. Rubenstein, *The concept privacy and its biological basis.* Journal of social Issues, 1977. **33**(3): p. 52-65.

[24] Posner, R.A., *The economics of privacy.* The American economic review, 1981. **71**(2): p. 405-409.

[25] Featherman, M.S. and P.A. Pavlou, *Predicting e-services adoption: a perceived risk facets perspective.* International journal of human-computer studies, 2003. **59**(4): p. 451-474.

[26] Dinev, T., et al., *Privacy calculus model in e-commerce–a study of Italy and the United States.* European Journal of Information Systems, 2006. **15**(4): p. 389-402.

[27] Huberman, A., M. Miles, and J. Saldana, *Qualitative data analysis: A methods sourcebook*. 2013, Thousand Oaks, CA: Sage Publications Inc.

[28] Flick, U., *An introduction to qualitative research*. 2018: Sage Publications Limited.

[29] Bauer, R.A., *Consumer behavior as risk taking.* Chicago, IL, 1960: p. 384-398.

[30] Plachkinova, M., A. Vo, and A. Alluhaidan, *Emerging trends in smart home security, privacy, and digital forensics*, in *Twenty-second Americas Conference on Information Systems*. 2016: San Diego.

[31] Gewald, H., K. Wüllenweber, and T. Weitzel, *THE INFLUENCE OF PERCEIVED RISKS ON BANKING MANAGERS'INTENTION TO OUTSOURCE BUSINESS PROCESSES: A STUDY OF THE GERMAN BANKING AND FINANCE INDUSTRY.* Journal of Electronic Commerce Research, 2006. **7**(2).

https://doi.org/10.30844/wi_2020_l5-haug

[32] Lei, X., et al. *The Insecurity of Home Digital Voice Assistants-Vulnerabilities, Attacks and Countermeasures*. in *IEEE Conference on Communications and Network Security (CNS)*. 2018.

[33] Wirth, J., C. Maier, and S. Laumer. *The Influence of Resignation on the Privacy Calculus in the Context of Social Networking Sites: An Empirical Analysis*. in *Proceedings of the Twenty-Sixth European Conference on Information Systems*. 2018. Portsmouth, UK.

[34] Edwards, A.L., *The social desirability variable in personality assessment and research.* 1957.

https://doi.org/10.30844/wi_2020_l5-haug