L. Hernández Acosta and D. Reinhardt. Smart Speakers and Privacy: Users' Perspectives. VDE dialog - The Technology Magazine, 04:8–10. 2020.

Smart Speakers and Privacy: Users' Perspectives

Luca Hernández Acosta
Computer Security and Privacy (CSP)
University of Göttingen
Göttingen, Germany
hernandez@cs.uni-goettingen.de

Delphine Reinhardt
Computer Security and Privacy (CSP)
University of Göttingen
Göttingen, Germany
reinhardt@cs.uni-goettingen.de

***Abstract*—The popularity of smart speakers and voice assistants in home appliances has considerably increased in the past few years. While smart speakers are convenient to use and provide useful features, their utilisation however raises privacy issues and users' concerns. These concerns are mainly related to the "always listening" nature of these devices and the potential misuse of personal data by companies, governments, and attackers. Such privacy concerns can impact the users' adoption and acceptance. Within the scope of this article, we therefore provide an overview of two studies conducted in the USA that analyse how different users feel about the use of smart speakers and investigate their understanding on how a smart speaker is treating their personal information, before identifying future research directions.**

***Index Terms*—Smart Speaker, Voice Assistants, Privacy**

Voice assistants are software-based solutions that allow hands-free interactions. They rely on (audio) speech data analysis. To activate them, users usually need to pronounce a wake-up word. After having recognised it, the voice assistants are then able to record and process the subsequent commands [1]. These voice assistants can be integrated in multi-function devices, such as smartphones, or be dedicated devices, so-called *smart speakers*. Apple was the first to integrate a voice assistant named Siri in an iPhone in 2011 [2]. In addition to Siri, examples of voice assistants available in Germany include Google Assistant, Alexa provided by Amazon, Cortana by Microsoft, and Bixby by Samsung [3].

As depicted in Fig. 1, the worldwide market for smart speakers has constantly evolved between 2016 and 2019. While the smart speaker market was originally controlled by Amazon in 2016, new global vending manufacturers have joined the market over time. In 2017, Amazon was still leading the market, but with a share of 52% only, as compared to the 88% of the year before. The same year Google was able to claim a 36% share of the market. In 2019, the smart speaker market was divided among multiple companies. Nevertheless, Amazon (28%) and Google (25%) remained the leading smart speaker manufacturers followed by Chinese manufacturers, including Baidu (11%), Alibaba (10%) and Xiaomi (8%). This means that Chinese manufacturers had a total market share of at least about 29%. In comparison, Apple had a smaller market share with 5%. Note that out of these assistants, the three most used in Germany are Alexa, Google Assistant, and Siri [3].

Asia shows the highest acceptance rate followed by the USA and Europe [3]. Among the European countries, Germany is below the average acceptance rate, while Italy, Spain, and the United Kingdom are leaders in the adoption of smart speakers [3]. However, in the past, similar acceptance rates could be observed in Germany for newly introduced technologies, such as smartphones and tablets. An increase in smart speakers' sales seems therefore possible in the near future [3]. Despite different acceptance rates, users of smart speakers in Germany and the USA have been shown to ask smart speakers to execute similar commands, the preferred ones being to play music and control other smart home devices [3]. Others tasks leveraged in different countries include web searches, weather forecasts, and setting timers and reminders [3].

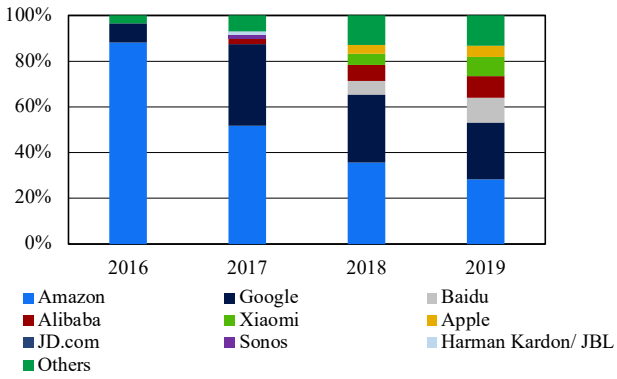

Fig. 1. Worldwide market share of smart speakers based on [4]

I. Common Architecture

While different models of smart speakers exist on the market, most of them are organised according to the same architecture shown in Fig. 2. This architecture includes three main components: (1) The smart speaker itself, (2) a cloud service, and (3) companion applications that can be installed on various different devices (e.g., smart phones or computers). The smart speaker records the user's voice and sends it to its cloud service, where the audio sample is processed. Depending on the command that a user has previously given as input, the cloud service sends a response to the smart speaker, which gives a vocal feedback to the user, or to the companion applications that need to perform a specific task. Like for the architecture, most current smart speakers are able to execute the same set of tasks. Recall that the most used tasks are searching the Internet, setting alarms and reminders,

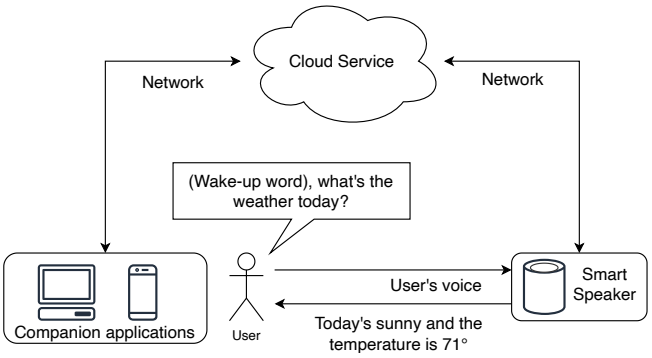

Fig. 2. Smart speaker architecture based on [6]

controlling other smart devices in the users' household as well as playing music [3]. Furthermore, third-party applications can be installed to extend the functionality of smart speakers. For example, these applications are referred to as *skills* for Alexa and *actions* for Google Assistant. By using them, users can be assisted when, e.g., learning and preparing for exams, working out, or helping children to properly brush their teeth [5]. As a result, most users leverage smart speakers for entertainment purposes at home.

II. Threats to Privacy

As already mentioned, existing smart speakers are listening for their wake-up word in order to be able to respond to users' commands. They hence collect audio samples of a few minutes before their activation as well as the commands themselves. This continuous listening raises privacy concerns for both users and non-users. The main users' concerns are related to their uncertainty on how data is collected, where it is stored, and how the data is processed [7]. In contrast, non-users do not want to use smart speakers because they believe that companies like Amazon and Google already gather a lot of their data and that they are not willing to provide additional personal information by using smart speakers [7].

The primary goal of this data collection is obviously to be able to execute the users' command. Besides, the collected data can be used to improve the provided services based on further analyses of the collected audio samples to, e.g., detect conditions under which the voice assistants have not been able to provide satisfactory answers to the users. Since smart speakers record users' commands, they gain insights about the users that can be used for both advertisement and profiling [8]. These insights include users' current search interests, grocery lists, shopping activities, or routines [8]. In the recorded samples, further insights about the users' context can be gained. For example, the current level of noise or the presence of other people. According to [8], additional inferences about the users' health and psychological status using data collected by their smart speakers may be possible in the future.

In addition to the threats to privacy related to the collection of audio samples, additional information about users can be gained by external adversaries based on an analysis of the communication patterns between the smart speaker and the cloud service or further devices installed in the same household, even if the traffic is encrypted [9]. For example, analysing the network activity and connections to cloud services can reveal when a smart speaker is used [10]. While the content remains encrypted, knowing the frequency at which smart speakers are used still provides information about users' habits.

III. Users' Perspective

To be able to address users' privacy concerns and design privacy-preserving solutions tailored to the users' needs and capabilities, we believe that it is necessary to first better understand how users feel about the use of smart speakers and investigate their understanding of how smart speakers are leveraging their personal information. While such understanding appears necessary to later foster users' acceptance, only two studies have been recently conducted in the USA, namely [11] and [7]. In what follows, we therefore report the key findings of both studies. Note that privacy is however known to depend on users' culture. This means that the obtained results may not be directly transferable to Germany. Further cross-cultural studies are therefore needed. The first study [7] counts 34 users as well as non-users and follows a qualitative approach. In contrast, the second study [11] conducted using a browser extension involves 103 participants.

As already shown in other contexts, participants in the second study [11] claimed that they have "nothing to hide". Even though some users question their privacy protection, the majority are rather careless when considering their own privacy [7], [11]. Users often tend to trade their privacy against the convenience that comes along with the use of smart devices. Some users restrict the use of smart speakers to non-sensitive topics and mute the device in case of sensitive situations. Topics perceived as sensitive include financial and sexual aspects as well as revealing information about their identity and whereabouts. Even if participants thought that the device is always listening to them, some users felt insecure about smart speakers being activated without their consent. They expressed the feeling of being uneasy and being monitored [11]. Among the recordings analysed in [11], about 10% did not resulted from an explicit user interaction.

However, it seems that missing knowledge about the smart speakers' underlying technology and functionalities can be a potential explanation for their preliminary lack of concerns. Indeed, about half of the participants in [11] did not know that their recordings are indefinitely stored by the provider. When confronted with this fact, some of them were surprised and would prefer shorter storage periods [11]. In [7], the users of smart speakers were not really concerned about the storage of their recordings, especially young participants were aware of it. Non-users expressed concerns about long storage periods, though.

When considering the functionality of reviewing and deleting recordings in [11], not all users knew about it. About half

of them found recordings containing the voice of people not belonging to their households and 25% did not feel comfortable in front of this discovery. Some users were also surprised and shocked to find the voice of their children or grandchildren in the recordings. In this situation, users were feeling very protective and wanted to delete these recordings, as they did not want their children's voice be stored on any server of a company. The same behaviour can be observed in presence of guests and the recording of conversations considered as private. Noteworthy, some users stated that they would like to keep most of the recordings because they believe that the data will be used to improve the smart speaker technology and to create voice profiles to be better understood by the device. In contrast to the reviewing function, even fewer participants knew that they could delete recordings and about 8% did already make use of this option.

Furthermore, participants in [11] did not want their data to be used for advertising purposes or by third parties. Nevertheless, few users had the impression that online advertisements they saw were based on private conversations that they had at home, thus suggesting that providers are using the recordings to trigger more personalised advertisements. What providers actually do with the recordings still remains opaque for some users [11].

In conclusion, current users of smart speakers were not frightened to keep using their smart speakers despite potential discoveries made during the study conducted in [11]. Nevertheless, they simultaneously indicated that they would appreciate improved and more intuitive privacy controls [11], thus laying the ground for future research in this area.

IV. Conclusion and Future Research Directions

The number of smart speakers sold in the world continuously increases. More and more users benefit from a simplified form of interaction with their devices to, e.g., control other smart home devices or play music. Although this convenience comes with a trade off with users' privacy, these adopters still feel comfortable when using smart speakers in their home. Even though controls are implemented by manufacturers to protect their privacy, users are often not aware of them. Nevertheless, users often feel relieved when learning about these privacy controls and expressed their ambition to use them to, e.g., delete stored recordings that they felt uncomfortable with. This however does not mean that the current situation cannot be further improved. For example, the current results show that users do not know existing privacy controls and are therefore not taking advantage of them. Hence, it is essential to better advertise these controls to the users. Moreover, the current privacy controls are manually configured by the users. To reduce the associated overhead, one possible approach could be to analyse users' privacy preferences to predict their privacy control settings. In the current state-of-the-art, it is further unclear for the users for which purposes the data are collected and which inferences may be made based on these recordings. Providing more transparency would be beneficial and may help them in making informed decisions about the overall utilisation of smart speakers or the utilisation of existing as well as future privacy controls. As a result, this research field is still in its infancy and additional efforts are necessary not to only better understand users' relationships with existing smart speakers, e.g., across different cultures, but also provide better ways of helping them in protecting their privacy.

References

[1] H. Chung, M. Iorga, J. Voas, and S. Lee, "Alexa, Can I Trust You?" *Computer*, vol. 50, no. 9, pp. 100–104, 2017.

[2] M. B. Hoy, "Alexa, Siri, Cortana, and More: An Introduction to Voice Assistants," *Medical reference services quarterly*, vol. 37, no. 1, pp. 81–88, 2018.

[3] S. Taş, C. Hildebrandt, and R. Arnold, "Sprachassistenten in Deutschland," WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH, Tech. Rep., 2019.

[4] Statista. (2019) Smart Speaker With Intelligent Personal Assistant Quarterly Shipment Share From 2016 to 2019. Accessed on 23-April-2020. [Online]. Available: https://www.statista.com/statistics/792604/worldwide-smart-speaker-market-share/

[5] B. Blass, "Wie Alexa & Co. den Alltag verändern," *Der Freie Zahnarzt*, vol. 62, no. 11, pp. 42–44, 2018.

[6] H. Chung, J. Park, and S. Lee, "Digital Forensic Approaches for Amazon Alexa Ecosystem," *Digital Investigation*, vol. 22, pp. S15–S25, 2017.

[7] J. Lau, B. Zimmerman, and F. Schaub, "Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviors With Smart Speakers," *Proceedings of the ACM Conference on Human-Computer Interaction*, vol. 2, pp. 1–31, 2018.

[8] A. Logsdon Smith, "Alexa, Who Owns My Pillow Talk? Contracting, Collaterizing, and Monetizing Consumer Privacy Through Voice-Captured Personal Data," *Catholic University Journal of Law and Technology*, vol. 27, no. 1, pp. 187–226, 2018.

[9] N. Apthorpe, D. Reisman, and N. Feamster, "A Smart Home Is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic," *arXiv preprint arXiv:1705.06805*, 2017.

[10] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, and N. Feamster, "Spying on the Smart home: Privacy Attacks and Defenses on Encrypted IoT Traffic," *arXiv preprint arXiv:1708.05044*, 2017.

[11] N. Malkin, J. Deatrick, A. Tong, P. Wijesekera, S. Egelman, and D. Wagner, "Privacy Attitudes of Smart Speaker Users," *Proceedings on Privacy Enhancing Technologies*, vol. 2019, no. 4, pp. 250–271, 2019.