**Smart Speakers: Can They Be Trusted?**

Faris Sahawneh, Murray State University

# Abstract

Smart speakers always remain in listening mode. As smart devices, they link back to servers and, with the help of smart assistants, wait for commands to begin interaction. The fact that smart speakers remain in listening mode forever means they continue to gather data about their surroundings even if no command is issued. It is possible to tell who someone is by listening to what is discussed. As such, smart speakers gather adequate information about people’s lives to create a profile about them. Tech companies actively collect data about their clients. At times, the government makes use of this information. Other people using the same smart speaker can also access personal information that does not belong to them. The people using smart speakers have minimal control over how their personal collected data is used and by whom. However, part of the reason smart speakers raise the privacy concern comes from the inadequate accountability by clients. People use smart speakers but do not take the time to review the privacy guidelines and learn about the privacy features. This research indicates that privacy protection tendencies are not expected. People who use smart speakers and other devices for smart homes that use the Internet of Things (IoT) keep from taking part in social, technical, and data-linked privacy safeguard behavior frequently. With people paying inadequate attention to privacy and how to ensure their smart speakers do not listen to them when not activated, the question arises as to just how much these devices take in without the user’s knowledge and consent.

# Introduction

There is fast progress with the Internet of Things (IoT). There are intelligent systems constantly making their way into daily lives and people’s households. However, with such devices, people also increase their concern about what intricate information is gathered and how this data is used (Guhr, Werth, Blacha, & Breitner, 2020). Unluckily, the role played by privacy is still significantly unchartered in the setting of smart homes.

Smart speakers are part of the IoT technologies in smart homes. Smart speakers are mobile devices that function on voice regulation using artificial intelligence and normal language processing to enable various hedonic and functional responsibilities like reminders, playing music, and obtaining data (Lau, Zimmerman, & Schaub, 2018). In most cases, the smart speaker is found in homes and buried deep in a whole smart home network. Smart speakers are, by the day, growing to be mainstream. In the United States, the adoption rates of smart speakers are high. As of December 2018, 66 million units were purchased (Feiner, 2019). Aside from the U. S., Europe also registers a convincing number in adopting smart speakers. In 2018, statistics indicated that smart speakers were available in 15.8 million European households (Cannizzaro, Procter, Ma, & Maple, 2020). The international market for smart speakers is projected to triple by 2023.

Smart speakers operate constantly. They remain in a listening mode waiting for audio acknowledgment with a chosen phrase or word from the smart homeowner (Guhr, Werth, Blacha, et al., 2020). Upon hearing the word, the smart speaker then actuates and starts interacting with the person. Upon activation, the transmission of lie audio information using Wi-Fi to third parties for processing and storage begins (Guhr, Werth, Blacha, et al., 2020). The fact that smart speakers are always on results in a significant privacy risk.

Research indicates that privacy protection tendencies are not common. People who use smart speakers and other devices for smart homes that use the IoT keep from taking part in social, technical, and data-linked privacy safeguard behavior frequently. There are additional and recent discussions on privacy indifference and cynicism (Choi, Park, & Jung, 2018). With people paying inadequate attention to privacy and how to ensure their smart speakers do not violate it, the question arises as to just how much these devices store without the client’s knowledge.

# Research Question

On privacy matters, are smart speakers listening in without the user’s knowledge?

# Literature Review/Theoretical Literature Review: Social Construction of Technology Theory

Technology displays an intricate bond with social circumstances. According to Sillar (1996), technology is associated with human emotions, enabling the use of artifacts and objects. Human feelings have a significant role in the association between technology and human beings. The sociological viewpoint in innovation study examines how the social framework affects the procedure and products of an innovative effort (Youseffikhah, 2017). The sociology of technology goes beyond applying theories and the frameworks of the sociology of science and technology. Concerning the technology determinism perspective, the link between technology and society is that the two are distinct spheres and technical modifications take place freely in the confines of the technological domain. In this perspective, society lacks an impact; however, technology impacts society and defines the development course (Elle, Dammann, Lentsch, & Hansen, 2010).

The Social Construction of Technology theory states that human events determine technology. With the construction of the technology determinism theory, there is a notion that technology shapes human events and technology due to the political, social, cultural, and economic setting (Burns, Corte, & Machado, 2016). People who are in support of this concept identify as social constructivists. Social constructivists believe that technology is hard to understand without the comprehension of the social setting. This framework in the confines of the science and technology studies sector has links to the sociology of science. The theory reacts to the technological determinism that recognizes technology as the shaper of human events (Burns, Corte, & Machado, 2016).

The idea of innovation is still intangible and vague. However, the term innovation can be defined from the standpoint of sociologists with the concept that points to the new organizational procedures and sequences and new services and products (Dahlin, 2014). The sociological perspective in the study of innovation focuses on how social structures affect the products as much as the process of innovative activity (Dahlin, 2014). Sociology of innovation pinpoints the characteristic of innovation and its structural configurations like social organizations, networks, and institutions that impact innovation.

There is an established link between sociology and technology and its innovations. This theory explores how social characteristics affect technology, like smart speakers, how they develop, and how they are used to gather information.

# Empirical Literature Review: Companies Listen to their Clients

There are many reasons why tech corporations like Google or Facebook choose to listen to what people say to their smart devices. The tech corporations need to assess samples from the population that uses their products (Molla, 2019). User conversations give these companies adequate room to capture what they need. From the conversations, the tech companies can improve upon the weak points of their products to benefit the client base. Workers from tech companies take time to listen to such conversations, taking note of keywords to arrive at informed perceptions concerning the client’s needs and market trends. Nonetheless, the samples used by the tech companies from the client population maintain anonymity (Molla, 2019). There is no way of tying analyzed data back to a particular client.

However, this does not offer any assurance. By listening to what someone is saying or talking about, it is possible to develop a background file on them and determine who they are. Smart speakers are private-sensitive IoT devices (Malkin, Deatrick, Tong, Wijesekera, Egelman, & Wanger, 2019). Every smart home device can bring to light data concerning the habits of its owners. Nonetheless, studies indicate that people think of two types of information that count as sensitive: videos and audio recordings from home. Smart speakers work with smart assistants, which act as the brains for voice technology for Siri, Alexa, and many others (Molla, 2019). These smart assistants remain on the lookout, waiting for their wake word to act as an activation to begin recording and transmitting data to servers. After transmission to the servers, the smart assistants gauge the best way to react to whatever prompts they are issued.

There is a constant fear that people’s phones continue listening in on what they say even when people are not speaking directly to them. Close to 43% of people who own smartphones believe that their mobile phones record what they say without their consent (Molla, 2019). Part of the notion that smart devices listen in on people without their permission comes from the content peddled by advertisers. Advertising content seems to always relate to what people think about it. Even though there is no factual proof that smart devices listen in without consent, signs are present.

# Personalization of Preferences in Daily Choices

Smart speakers can personalize the owners’ preferences. This personalization takes place without specific instructions from the owner of the smart speaker. Smart assistants embedded within the servers of these smart speakers take note of keywords to determine what the owners like and dislike. People in the U. S. who have smart speakers display mixed sentiments concerning the importance of smart speakers in personalizing their preferences. According to Auxier (2019), close to one in every five people who own smart speakers, amounting to 18%, indicate that smart speakers must consider their preferences and interests when reacting to queries and instructions. Thirty-eight percent of people who own smart speakers suggest that it is somewhat critical for smart speakers to do the same (Auxier, 2019). Close to four in every ten people in the U. S. who have smart speakers indicate that it is not essential for smart speakers to personalize what they want.

Many people who own smart speakers do not wish to attain additional personalized services. Fifty-eight percent of respondents in a Pew Research Center study indicated they do not want their smart speakers to improve their preferences and interests (Auxier, 2019). The other 42% want the opposite. The research added another important finding about looking for information. When people were asked whether they would agree to personalization, even if it meant the smart speakers had to gather additional personal data, 66% of the respondents did not agree with the idea (Auxier, 2019).

Smart speakers can personalize their services using the 2019 study from Pew Research Center as a pointer. However, to personalize their products and services, smart speakers take the initiative to gather additional personal data from the customers. In collecting this information, there is no guarantee that the owner’s consent is sought—this lack of assurance results in a breach of privacy.

Smart speakers have a built-in automatic speech recognition (ASR) system to facilitate natural communication between the user and the device. Smart speakers are always on and constantly recording their surroundings for ease of use. The speaker should only respond to a specific trigger, hot or trigger word. However, in their research, as seen in Figure 1, Schönherr, Golla, Eisenhofer, Wiele, Kolossa, & Holz (2020) discovered that local and cloud ASR engines have misrecognized many accidental triggers.

Figure 1: Cloud VS. local ASR trigger recognition (Schönherr, Golla, eisenhofer, et al., 2020)

# Client Opinion on Privacy Issues

For most people using smart devices like smart speakers, the benefits go past their privacy concerns. However, the big question is whether people using smart speakers make informed choices. Is it possible that people fail to comprehend the consequences and regulations at their disposal fully? Users might not even know that their interactions go into a forever storage system controlled by the manufacturers of the smart speakers (Lutz & Newlands, 2021). Other people in the smart home can review personal interactions when they wish. Privacy is compromised, and the people involved are unaware of it.

In another study by Malkin, Deatrick, Tong, et al. (2019), it is clear that people have no idea that their interactions go into permanent storage. People are also unaware of the possibility of assessing their past interactions by retrieving stored information. Unsurprisingly, some people feel the data stored with voice assistants in smart speakers do not count as sensitive. However, people are dissatisfied with the prevailing retention guidelines. Overall, people disagree with the permanent storage of their information by smart assistants in smart speakers (Malkin, Deatrick, Tong, et al., 2019). Many people also find it unacceptable to review their information and interactions with smart assistants and manufacturers of smart speakers. Very few people agree that they employ the provided privacy characteristics of these smart speakers (Malkin, Deatrick, Tong, et al., 2019). People should take up proposals for privacy features like the automated deletion of recordings. All these findings and claims prove that people lack complete information on the behaviors of their smart speakers and the available privacy features.

In another report by Pew Research Center (Auxier, Rainie, Anderson, Perrin, Kumar, & Turner, 2019), there is conflicting information regarding people’s knowledge of the privacy concerns for their smart speakers. Many people in the U. S. believe that their online actions are regularly tracked and assessed by tech corporations. Six out of ten people believe that it is impossible to go through a typical day without some information about them being collected by smart devices for the benefit of the US Government or the involved tech companies (Auxier, Rainie, Anderson, Rainie, Anderson, et al., 2019). Many people in the US (79%) also register concern over how their information is used by these tech companies (Auxier et al., 2019). People indicate that they do not have adequate authority over how the government and tech companies use their data.

Americans' regard for digital privacy covers people who gather, store and use personal data. In addition, a significant percentage of the public lacks confidence in companies being good stewards of the information collected (Auxier, Rainie, Anderson, et al., 2019). Seventy-nine percent of people in the U. S. are not confident that tech companies will agree to make mistakes concerning the misuse and compromise of personal data. Sixty-nine percent are not satisfied that companies will not use their data in ways that bring discomfort (Auxier, Rainie, Anderson, et al., 2019).

Despite the American public harboring concern over several aspects of their digital privacy, the majority admit they lack diligence in attending to privacy guidelines and terms of services with products they use daily (Auxier, Rainie, Anderson, et al., 2019). Even though 97% of the American public agrees to be sought for consent on approval of privacy policies, close to only one out of every five adults agrees that they go through privacy policies before deciding to do the same (Auxier, Rainie, Anderson, et al., 2019). Thirty-eight percent agree that they read the policies before agreeing to the same, with 36% saying they never read before agreeing.

In essence, part of the problem with privacy regarding smart speakers stems from the fact that users are unaware of the privacy guidelines. People do not engage in learning about privacy and how they can safeguard themselves. Even though companies manufacturing smart speakers might have additional privacy features, not all people use these features. Part of the privacy issues arising from smart speakers listening in on owners come from ignorance and reluctance to fully comprehend device features and capabilities.

# Discussion

Smart speakers continue to be adopted by more households, becoming a mainstream technological invention. Smart speakers operate continuously, meaning they do not turn off unless there is an error with Wi-Fi and network connection. These smart devices maintain a listening mode awaiting audio recognition with a designated word from the owner. According to research, privacy safeguard behaviors are not regular for people using smart devices like smart speakers (Guhr, Werth, Blacha, et al., 2020). People using smart speakers like Alexa and Siri refrain from engaging in technical, social, and data-associated privacy protection behaviors. Part of the blame falls on the oblivious nature of the clients.

The Social Construction of Technology theory explains how society interacts with technology. According to the theory, human actions determine technology’s course (Youseffikhah, 2017). Social features impact the technology of smart speakers in determining their development, improvements, and how they collect information about their users. The theory can also be used to understand why tech companies providing smart speaker services and products choose to listen in on their customers. These tech companies need to evaluate population samples concerning the use of their products.

Smart speakers can personalize people’s preferences, but most people using smart speakers do not choose to personalize their experience. To customize preferences, smart speakers take in personal data, which can be acquired without consent from the client. In the long run, privacy is breached. People do not have complete control over the information gathered and stored by their smart speakers (Auxier, 2019). The government and tech companies can access and use this information. Other people with access to smart speakers can review personal data that does not belong to them. With the use of smart speakers, there are many ways privacy is compromised, and clients are not even aware.

Even though people express worry over different perspectives of digital privacy, many agree that they do not have the diligence to address privacy guidelines and terms of service on products. A significant part of the challenge in using smart speakers is that privacy is compromised because clients do not know about privacy features and guidelines, and even those who know about them do not take the initiative to use them.

# Conclusion and Recommendations

Smart speakers always remain in listening mode. As smart devices, they link back to servers and, with the help of smart assistants, wait for commands to begin interaction. The fact that smart speakers forever remain in listening mode means they continue to gather data about their surroundings even if a command is not issued. It is possible to identify a person by listening to their conversations. As such, smart speakers gather adequate information about people’s lives to create a profile. Tech companies actively collect data about their clients. At times, the government makes use of this information. Other people using the same smart speakers can also access personal information that does not belong to them. The people using smart speakers have minimal control over who collects their data and how it is used. However, part of the reason smart speakers raise the privacy concern comes from the inadequate accountability by clients. People use smart speakers but do not take the time to review the privacy guidelines and learn about the privacy features.

Few countermeasures can be used to address the privacy concerns of smart speakers. Users of smart speakers rely on the voice channel for communication, which creates a vulnerability. Using biometrics to identify the device owners is a valid defense against such weakness in smart speakers. Another approach is to allow the users to customize their own wake words. For example, users can repeatedly repeat the wake word, saying, “Alexa, Alexa, Alexa.” Future research is needed to help find more countermeasures to safeguard the privacy concerns of smart speaker users.

# References

Auxier, B. (2019, November 21). 5 things to know about Americans and their smart speakers. Retrieved from https://www.pewresearch.org/fact-tank/2019/11/21/5-things-to-know-about-americans-and-their-smart-speakers/

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Retrieved from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Burns, T. R., Corte, U., & Machado, N. (2016). The sociology of creativity: PART III: Applications–The socio-cultural contexts of the acceptance/rejection of innovations. *Human Systems Management, 35*(1), 11-34. doi: 10.3233/HSM-150852

Cannizzaro, S., Procter, R., Ma, S., & Maple, C. (2020). Trust in the smart home: Findings from a nationally representative survey in the UK. *PLoS ONE, 15*(5). doi:10.1371/journal.pone.0231615

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior, 81*, 42-51. doi:10.1016/j.chb.2017.12.001

Dahlin, E. C. (2014). The Sociology of Innovation: Organizational, Environmental, and Relative Perspectives. *Sociology Compass, 8*(6), 671-687. doi: 10.1111/soc4.12177

Elle, M., Dammann, S., Lentsch, J., & Hansen, K. (2010). Learning from the social construction of environmental indicators: From the retrospective to the pro-active use of SCOT in technology development. *Building and Environment, 45*(1), 135-142. doi: 10.1016/j.buildenv.2009.05.011

Feiner, L. (2019, February 5). Apple’s smart speaker is struggling against rivals from Amazon and Google. Retrieved from https://www.cnbc.com/2019/02/05/apple-homepod-smart-speaker-market-share.html

Guhr, N., Werth, O., Blacha, P. P. H., & Breitner, M. H. (2020). Privacy concerns in the smart home context. *SN Applied Sciences, 2*(247), 1-13. doi:10.1007/s42452-020-2025-8

Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, are you listening? Privacy perceptions, concerns, and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction*, *2*(102), 1-31. Retrieved from https://dl-acm-org.proxyiub.uits.iu.edu/doi/pdf/10.1145/3274371. doi: 10.1145/3274371

Lutz, C., & Newlands, G. (2021). Privacy and smart speakers: A multi-dimensional approach. *The Information Society, 37*(3), 147-162. doi:10.1080/01972243.2021.1897914

Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Egelman, S., & Wagner, D. (2019). Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies, 2019*(4), 250-271. doi:10.2478/popets-2019-0068

Molla, R. (2019, September 20). Your smart devices listening to you, explained. Retrieved from https://www.vox.com/recode/2019/9/20/20875755/smart-devices-listening-human-reviewers-portal-alexa-siri-assistant

Schönherr, L., Golla, M., Eisenhofer, T., Wiele, J., Kolossa, D., & Holz, T. (2020). Unacceptable, where is my privacy? exploring accidental triggers of smart speakers. *arXiv preprint arXiv:2008.00508*.

Sillar, B. (1996). The dead and the drying: Techniques for transforming people and things in the Andes. *Journal of Material Culture, 1*(3), 259-289. doi: 10.1177/135918359600100301

Yousefikhah, S. (2017). Sociology of innovation: Social construction of technology perspective. *Ad-Minister*, *30*, 31-43. doi:10.17230/ad-minister.30.2

Biography

FARIS SAHAWNEH is an assistant professor at Murray State University in the Cybersecurity and Network Management program. Dr. Sahawneh received his M.S in Telecommunications Systems Management from Murray State University and his Ph.D. in Business Administration with a specialization in Computer and Information Security from Northcentral University. He has extensive experience in cybersecurity, forensics, and servant leadership, and his interests include IoT, virtualization, cyber ethics, and digital privacy. Dr. Sahawneh may be reached at fsahawneh@murraystate.edu