Abstract

The aim of this study was to assess privacy and data protection concerns among smart speaker users versus non-users and determine suitable strategies to mitigate any occurring deterrents by the means of corporate digital responsibility (CDR) measures. The current state of research on this topic includes qualitative interview findings, with major concerns on the topic of data protection risks such as unauthorized voice recordings, hacker attacks or improper use of user data obtained through smart speaker usage being point of discussion.

The current state of research also includes studies that specifically address technical limitations of this technology. After a thorough literature research, no quantitative studies could be found that address the privacy concerns and barriers of smart speaker users in comparison to non-users and elaborate on specific strategies to reduce these barriers and deterrents among the two sub-groups. This study focuses on initial CDR models and subsequently highlights how a company's values and norms around CDR can be translated into practicable guidelines to alleviate usage barriers of smart speakers. This is intended to both demonstrate practical implementation options for relevant stakeholders as well as further incentivize future research related to CDR readiness, implementation, and success.

Based on the literature review, the following research questions were addressed through a quantitative online survey of consumers and potential consumers of smart speakers:

a) Do non-users of smart speakers have higher privacy barriers than individuals who already use smart speakers?
b) Which proposed CDR measures can stakeholders use to mitigate possible privacy barriers?

The results of this quantitative study have not yielded significant differences in the strength of privacy concerns between non-users and users of smart speakers. However, data privacy concerns were raised amongst both sub-groups of the study. On one hand, current users of smart speakers responded significantly better to the possible implementation of CDR measures to mitigate the above-mentioned concerns. On the other hand, non-users also showed promising potential to respond to CDR strategies as a measure to reduce data privacy-related barriers of smart speaker usage.