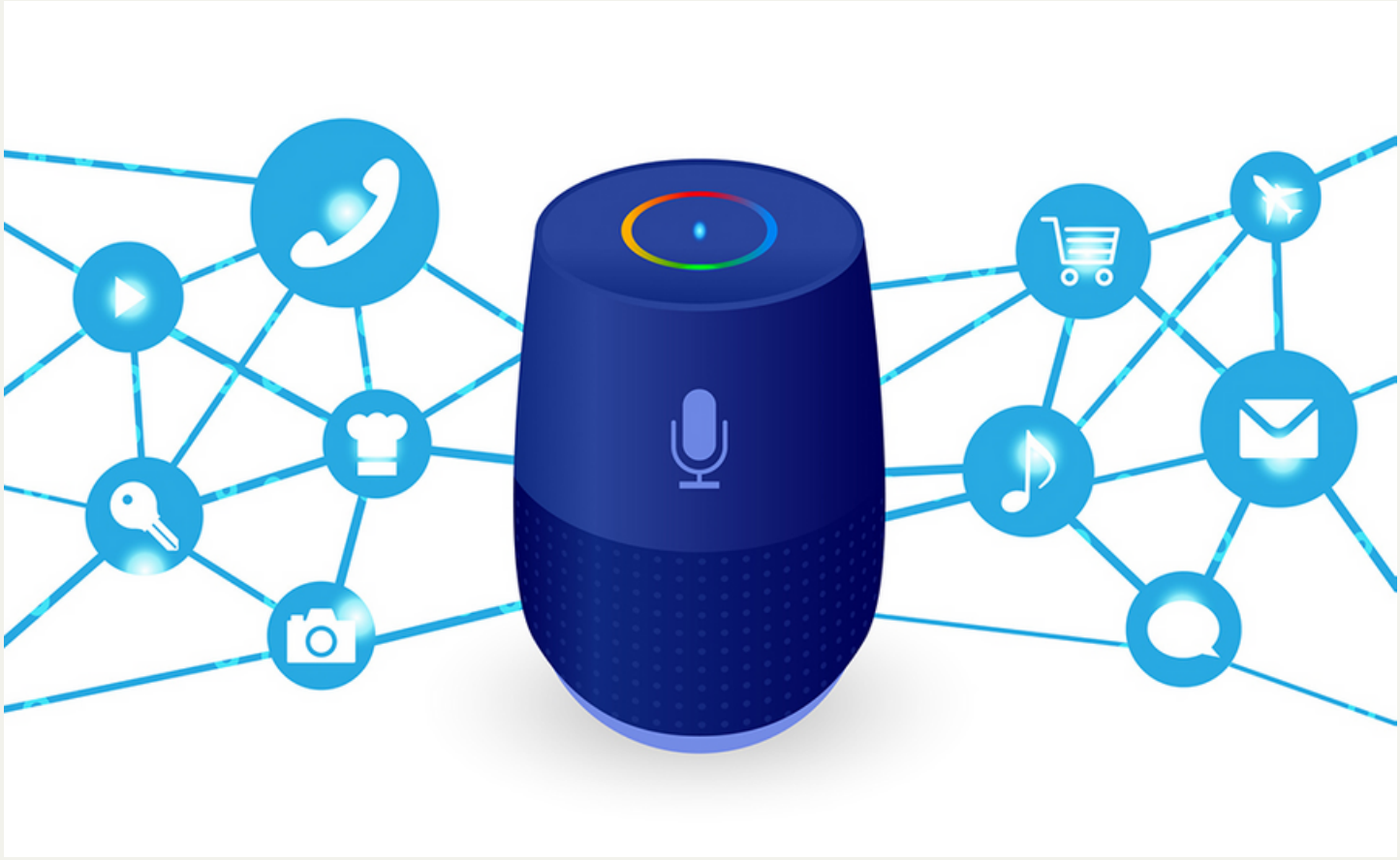
MASTER THESIS

PRIVACY IN THE AGE OF IOT

An experimental study investigating the attitude towards smart speakers of non-owners through voice activation and data evaluation as intrusive features



HEDDA PALENIO

AUGUST 2020

UNIVERSITY OF TWENTE.

Examinationcommittee:
Dr. M. Galetzka
Prof. Dr. M. T. D. de Jong

Privacy in the Age of IoT

An experimental study investigating the attitude towards smart speakers of non-users through voice activation and data evaluation as intrusive features

Master Thesis

Student name: Hedda Palenio
Student number: s15409550
E-Mail: h.l.palenio@student.utwente.nl

University: University of Twente
Faculty: Behavioural Management and Social Science (BMS)
Study Program: Communication Science
Specialization: Digital Marketing Communications

Supervisors: Dr. M. Galetzka and Prof. Dr. M.T.D. de Jong

Date: August 27, 2020

UNIVERSITY OF TWENTE.

Abstract

Purpose: Ownership of smart speakers all around the world is rising. The devices with voice assistants provide a lot of convenience and autonomy to users. However, consumers often ignore the privacy issues for the benefits the smart speakers offer. This research aims to address this topic in investigating how intrusive technology features like unintentional voice activation and data evaluation by humans influence the attitude towards smart speakers. Additionally, mediating and direct effects of perceived usefulness, privacy concerns, and trust should be tested.
Method: As a method, an experiment including a fictive scenario was conducted to test the proposed model. Therefore, a 2 (unintentional vs. intentional voice activation) x 2 (data evaluation by software vs. by humans) between-subject experiment was set up to investigate the intrusive effects of unintentional voice activation and data evaluation by humans on perceived usefulness, privacy concerns, trust, and attitude towards smart speakers. The target group of the experiment were non-owners of smart speakers (n=186).
Results: The results of the MANOVA analysis showed that there were no significant effects of voice activation and data evaluation on attitude towards smart speakers, trust, and privacy concerns. However, a marginally significant effect of data evaluation on perceived usefulness was found. Perceived usefulness was lower if data evaluation was done by software. Furthermore, a marginally significant interaction effect of voice activation and data evaluation on trust was found. In the intentional voice activation condition, trust was lower if data evaluation was done by software. Moreover, the analysis showed significant main effects of perceived usefulness, privacy concerns, and trust on attitude. Besides, no mediation effects of perceived usefulness, privacy concerns, and trust were found.
Conclusion: It seems that non-owners perceive the smart speaker to be more useful if data evaluation is done by humans (compared to software). Non-owners also give the impression that they differ in their level of trust if the smart speaker is activated intentionally depending on the type of data evaluation. Data evaluation by humans seemed to be regarded as more trustworthy than data evaluation by software if the smart speaker was activated intentional. In general, low perceived usefulness, low trust, and high privacy concerns lead to a negative attitude towards smart speakers. Findings can be used as an inspiration for future research in the growing field of IoT technology and are practically relevant for smart device developers and technology companies

Keywords: smart speakers, internet of things, privacy concerns, perceived usefulness, trust, attitude towards smart speakers

Table of Contents

1. Introduction

The Internet of Things (IoT) arrived in individuals' homes during a time in which smart home technologies are becoming increasingly popular all over the world (Brush, Hazas, & Albrecht, 2018). Such internet-connected devices run with sensors and offer various functionalities to manage and control other technologies in the household. They are designed to improve the home security and efficiency, as well as the comfort and entertainment of users in their daily life (Jacobsson & Davidsson, 2015).

Smart speakers are a prime example of an IoT device. They are the highest growing consumer goods in the technology sector (Perez, 2018; Pridmore, Zimmer, Vitak, Mols, Trottier, Kumar, & Liao, 2019). People often make their first contact with the smart home world via smart speakers with virtual assistants (Fruchter & Liccardi, 2018), the most popular of which are Amazon Echo with its virtual assistant Alexa and Google Home (Al-Heeti, 2019). By the end of 2018, there were probably around 100 Million smart speakers on the market. In the United States, 24 percent of households adopted a smart speaker in 2018 – a number which is expected to increase to 75 percent in 2020 (Olson & Kemery, 2019). The adoption rate in Europe is much lower, arguably because the market entry occurred later there. In Germany, for instance, 11 % of households use smart speakers in 2019 (Kinsella, 2019b), while in the Netherlands only 5% of the population adopted a smart speaker (Kinsella, 2019a).

At the same time, smart speakers are accompanied by privacy issues. Experts have warned about the vulnerability related to privacy issues that comes with the continuously listening microphones of smart speakers (Lau, Zimmermann, & Staub, 2018). But are users aware of this? Lately, many scandals such as the released news that Amazon employs thousands of workers listening to voice recordings of Amazon Echo increase consumers' awareness of the privacy risk accompanying such devices by consumers (Day, Turner, & Drozdiak, 2019). Confirming this heightened awareness, Olson and Kemery (2019), for example, state that 41 percent of smart voice assistant users have privacy concerns. This ranges from data security to passive listening concerns. Additionally, 24 percent of the users who participated in the study said that they do not know how their data is used (Olson & Kemery, 2019).

Benlian, Klumpe, and Hinz (2019) showed that intrusive features of smart speakers lead to privacy invasion and harm users need for privacy. In an experiment based on vignette scenarios with actual smart speaker owners they analyzed the effect of unintentional voice activation and anthropomorphic design on individual strain. They found that intrusive technology features cause strain and interpersonal conflicts. The findings in the study show that unintentional voice activation of smart speakers leads among others to concerns about security and privacy among smart speaker users. Another study by Malkin, Deatrick, Tong, Wijesekera, Egelman, and Wagner (2019) sheds light on the consumers' differing perception of various

types of data evaluation. Participants in the study considered data evaluation by humans as unacceptable compared to data evaluation by machines. This shows that data evaluation by humans is an intrusive feature for smart speaker owners as well. However, only few studies investigating these intrusive effects on the perceptions of non-owners. Thus, further exploration into the effect of intrusive technology features is needed.

Besides, much research exists in the emerging domain of privacy concerns around smart technologies. Many authors concentrate on smart homes in general and examine various devices (Chhetri & Motti, 2019). Chhetri and Motti (2019) examined privacy concerns for smart home devices like Amazon Echo or Google Home from a user-centered perspective. Focusing on current users of smart home devices, the authors investigated different online reviews. They found that many users are concerned about privacy and classified the concerns into categories. The most frequently mentioned concerns were that smart speakers are always listen to conversations and that they track users' actions as well as preferences of users (Chhetri & Motti, 2019). Also, other studies from authors such as Menard and Bott (2018) examined privacy perceptions with a focus on users that have at least one smart home device. While analyzing the adoption decisions of smart home devices, the authors highlight associated privacy concerns which results from the adoption. Drawing on privacy calculus theory Princi and Krämer (2019) examined the effect of convenience and tracking capabilities of smart devices. They showed that tracking capabilities do not concern users of smart vacuum cleaners while convenience was a major success factor for the willingness to deploy those technologies. Besides, different studies suggest that trust has a positive effect on attitude and can mitigate privacy concerns (Worthy, Matthews, & Viller, 2016; Zheng, Apthorpe, Chetty, & Feamster, 2018).

In general, research on privacy concerns concentrates mostly on people who already use a smart speaker. The use of a smart device requires that the purchase decision was already made regardless of the privacy concerns. Presumably, the primary motivator for the purchase decision is the convenience or usefulness of smart speakers since they promise comfort and control and in some cases security and safety (Chhetri & Motti, 2019).

This raises the question of whether people who did not buy a smart speaker made this decision based on privacy reasons or for other reasons. What are non-users specifically concerned about and can those concerns lead to the decision of not purchasing a smart speaker? Or do the perceived benefits of smart speakers outweigh the concerns? And which role does trust play? Current literature lacks the answer to these questions for potential smart speaker owners. Although the various scandals show that it is a controversial topic, little research has been done focusing specifically on the case of smart speakers and consumers' concerns about privacy in relation to the benefits that the devices offer. Additionally, the target group of people who do not own a smart speaker (yet) is highly relevant as the examination of technology "non-

use" remains important (Baumer, Burrell, Ames, Brubaker, & Dourish, 2015). Addressing this research gap, the study posits the following research questions:

(RQ1): How do perceived usefulness, privacy concerns, and trust influence the attitude towards smart speakers of non-owners?

(RQ2): To what extent do voice activation and data evaluation influence the attitude of non-smart speaker owners?

(RQ3): To what extent is the effect of voice activation and data evaluation on attitude towards smart speakers mediated by perceived usefulness, privacy concerns, and trust?

To answer the research questions, a new model was created. The new model combines factors from the technology acceptance model and privacy calculus since this study aims to analyze the attitude towards smart speakers with regards to the privacy trade-off. Therefore, the following mediation variables were examined: privacy concerns, perceived usefulness, and trust as well as the dependent variable attitude towards smart speakers. The relationship between the variables was analyzed by means of an online survey which included a 2x2 between-subject experiment compromising a vignette-based scenario with two common intrusive features of smart speakers. The scenario aimed to introduce participants to intrusive technology features since potential owners probably have no in-depth knowledge about privacy issues related to smart speakers. In this study, these features are unintentional voice activation and data evaluation by humans because both are frequently addressed in critical articles dealing with the data protection of intelligent speakers (Hurtz, 2019; Zorn, 2020).

In the present research, only smart speakers are the point of interest. Voice assistants on mobile phones or computers such as Siri or Cortana and other technologies are not included due to distinctive differences in usage.

This study is relevant in theoretical and practical regards. It contributes to academic literature since the attitudes of non-smart speaker users have not been addressed before in the context of the technology acceptance and the privacy calculus model. In addition, it can educate what the provision of intrusive technology features does with the attitude towards technologies in humans. Furthermore, it might also have practical implications since knowledge about attitudes and concerns of potential consumers can help manufactures and policymakers to improve guidelines and privacy protection. Additionally, the study might also help potential consumers and society in raising awareness for and a deeper understanding of privacy issues related to smart technology devices.

2. Theoretical framework

2.1. Smart speakers in the context of IoT

The first smart speaker with an intelligent voice assistant (Amazon Echo) was released in 2015 (Jackson & Orebaugh, 2018). Recently, intelligent voice assistants are available everywhere. In homes, cars, and public services people get used to operating with technical devices through their voice (Malkin et al., 2019). Research states that it is only a matter of time until every possible device can be controlled by voice (Blass, 2018). Already today, about a quarter of technical devices users state that they prefer to communicate with conversation assistants rather than interacting with typed text input via apps or websites. These acceptance rates will probably increase rapidly in the next three years because intuitive voice input is easy to use and therefore convenient in everyday life (Rabe, 2019).

Smart speaker as an Internet of Things (IoT) device are a key instrument for the smart home. Hoffman and Novak (2015) describe smart products as devices that interact and communicate towards themselves but also towards others and humans using Internet data that is administered in a database, while working with intelligence, ubiquity, and autonomy. A smart speaker usually includes a virtual assistant that can be used for interactive actions with hands-free activation. Most smart speakers can also connect to WI-FI or Bluetooth. Smart speakers consist of microphones, speakers, and interfaces that enable consumers to play music, create to-do list, purchase products and services, search for online information, and manage other smart home devices (Kowalszuk, 2018). To use these various functions, the installment of small auxiliary programs is necessary. Such programs are called "Skill" on Amazon and "Actions" on Google (Blass, 2018).

The microphone of a smart speaker is constantly active in recording all requests of the user and offers hands-free voice control. To identify a command and to provide answers, the speaker continuously waits for the wake-word like “Ok Google” or “Alexa” (Lau et al., 2018). The requests and questions are sent to a server for analysis and evaluation of the data. Through this process, consumers get the feedback they asked for. The two most popular smart speaker brands are Amazon’s Echo/Alexa and Google Home/Google Assistant. Smaller brands are, for example, Alibaba, Sonos, and Apple whose HomePod entered the market in 2018 (Gordon, 2019).

2.2. The privacy trade-off for the attitude towards smart speakers

Attitude towards technology and eventual adoption can be affected by various factors (Rahim, Safin, Kheng, Abas, & Ali, 2016). This research generally concentrates on factors revolving around the term privacy. Therefore, different factors were combined from two models. First,

the privacy calculus model was used as a basis, adding the privacy trade-off to the study. Concentrating on the specific context of purchasing products and services, the privacy calculus model builds on behavior calculus theory (Majumdar & Bose, 2016). It proposes that an individual's intention to disclose personal information is based on a cost-benefit analysis (Smith, Dinev, & Xu, 2011). This privacy-related decision making is called privacy trade-off and is considered a rational process. It explains the willingness or intention to provide personal information in exchange for the benefit of a product or a service. In the privacy context, the costs relate to various personal information risks that evolve from disclosure (Majumdar & Bose, 2016).

The privacy calculus model is usually used in the context of social network sites (SNS), personalized advertising (Schumann, Wangenheim, & Groene, 2014) or mobile apps (Wottrich, Van Reijmersdal, & Smit, 2018). These studies show that users disclose personal information in exchange for free services on these websites. Regarding the special case of the Internet of Things which compromises smart speakers, personal data is collected without an active awareness of the user's consent. Thus, potential owners of smart speakers can only decide to use a smart speaker or not (Princi & Krämer, 2020). In this case, disclosure of personal information is to be equated with intention to adopt. In summary, the privacy trade-off aims to analyze if perceived privacy risks (privacy concerns) can be outweighed by perceived benefits (e.g. perceived usefulness).

The technology acceptance model (TAM) by Davis (1989) is an extension of the theory of reasoned action and predicts how users accept and use different technologies. Davis' model suggests that perceived usefulness and perceived ease of use influence an individual's attitude and eventually the behavioral intention to use a specific technology. Perceived usefulness and perceived ease of use can be affected by various variables depending on the kind of technology. The TAM was extended with other factors to increase explanatory power by additional models and theories. For example, the study of Dhagarra, Goswami, and Kumar (2020) add the effects of privacy concerns and trust to the TAM in healthcare and Zhang, Tao, Qu, Zhang, Lin, and Zhang (2019) extended the original model for automated vehicles with among others initial trust and perceived privacy risk.

2.3. Hypotheses development

2.3.1. Attitude towards smart speakers

According to the TAM, behavioral intention to use a technology is influenced by attitude as a general idea about the technology (Davis, 1989). In the present research, behavioral intention to use a technology is not included because non-users of smart speakers might have different reasons not to use the respective device. Instead, it was decided to focus on the attitude

towards smart speakers since it plays a major role in the process of accepting technology (Yang & Lee, 2018). This is supported by the study of Chhetri and Motti (2019) who claim that consumers positive attitudes lead them to utilize smart speakers. This outcome is also predicted by the privacy calculus model (Dinev, Albano, Atri, Xu, & Hart, 2016; Smith et al., 2011).

According to the privacy calculus model, consumers will disclose personal information, when engaging in a privacy trade-off and perceived benefits are at least balanced by, if not higher than, perceived privacy risks (Dinev et al., 2016). In the special field of smart technologies, this trade-off results in consumers' decision of either using a device or not. Since the utilization of a smart speaker requires a generally positive perception of the device, the attitude towards smart speakers is included in the present research as the dependent variable.

2.3.2. Perceived usefulness

Perceived usefulness is a key advantage for the acceptance of smart speakers. The term belongs to the TAM and has been analyzed in literature about ubiquitous computing (Yoon & Kim, 2007) and smart speaker adoption before (Kowalczuk, 2018; Yang & Lee, 2018). These studies found that perceived usefulness results in positive attitudes towards smart speakers. Perceived usefulness is a cognitive belief and defined as "the degree to which an individual believes that using a particular system would enhance his or her job performance" (Davis, 1989, p. 320). Smart speakers promise to have a lot of advantages for consumers. Overall, they offer increased autonomy through hands-free technologies and through their various functionalities. The efficiency and functionality of smart speakers can be summarized as perceived usefulness. Research found out that smart speaker users commonly accept the privacy trade-off because they value the high usefulness of the devices (Pridmore et al., 2019).

Perceived usefulness is highly related to the concept of perceived convenience, which is also analyzed in research about smart speakers before (Chhetri & Mottie, 2019; Zheng et al., 2018). Overall, those studies predict that convenience is the main reason of accepting privacy loss in the future. Princi and Krämer (2020) established that the willingness to deploy smart technology is influenced by the effect of convenience. The authors also used the privacy calculus model when analysing the effect of convenience and tracking on the intention to use a smart device. Zheng et al. (2018) highlight in their study that convenience is an important driver in the process of adopting smart speakers for consumers.

In addition to usefulness and convenience, the benefit of enjoyment is highlighted in existent literature as an influential factor of acceptance of the smart speakers (Kowalczuk, 2018; Pridmore et al., 2019). Kowalczuk (2018) defines perceived enjoyment as "the extent to which the use of smart speakers is perceived enjoyable in its own right" (p. 7). In a study of Yang, Yu, Zo, and Choi (2016), it was found that the enjoyment of wearable devices influences

the perceived value of these technologies. This outcome can apply to smart speakers as well. Also, in the context of smart speaker, personalized services are an important component. Personalization is a construct widely studied in marketing and consumer psychology. It causes the products and services that fit the customer based on personal data collection (Kim, Park, Park, & Ahn, 2018). An increased number of smart home users are building a personal relationship with their voice assistants. This goes hand in hand with the desire to personalize and individualize the digital companions more (Smirek, Zimmermann, & Beigl, 2016).

In the present study, perceived usefulness, convenience, enjoyment, and personalization are summarized under the term perceived usefulness since the concepts are highly connected. They all relate to the benefits provided by smart speakers. Convenience, enjoyment, and personalization symbolize specific benefits for the user, while usefulness is a more comprehensive term. This justifies the merge of the three terms to perceived usefulness. In relation to the privacy calculus model, the factor perceived usefulness stands for the perceived benefits which are of great importance for the privacy trade-off and ultimately determine the consumer's attitude towards the product.

(H1): High perceived usefulness positively affects the attitude towards smart speakers.

2.3.3. Privacy concerns

In internet technology literature, privacy concerns in ubiquitous computing have been an active subject of discussion (Zheng et al., 2018; Gerber, Reinheimer, & Volkamer). Privacy concerns are operationalized as consumers' beliefs, attitudes, and perceptions about their privacy (Smith, Milberg, & Burke, 1996). Thereby, privacy is defined as "the ability of the individual to control the terms under which personal information is acquired and used" (Westin, 1967, p.7). Privacy concerns may occur in the process of information disclosure to a certain external agent and are specified as concerns about possible loss of information (Wottrich et al., 2018). Research has shown that privacy concerns negatively influence consumers' willingness to share personal information on the internet as well as the intention to use online services (Fortes, Rita, & Pagani, 2017). Additionally, concerns related to privacy may affect attitudes towards the acceptance of technology (Menard & Bott, 2018). Previous studies of smart speakers found that privacy concerns are the primary reason for the non-adoption of those devices (Chhetri & Motti, 2019; Lau et al., 2018).

A common concern of users is that smart speakers always overhear conversations which results in a feeling of "creepiness". The home assistant is then seen as a "spy", but users still accept the surveillance as a trade-off for the convenience and functionality of their devices (Fruchter & Liccards, 2018; Primore et al., 2019;)

For most people, their home is a place where privacy is highly important. Especially oral conversations are considered private and normally nobody would like to have them digitally captured (Choe, Consolvo, Jung, Harrison, & Kientz, 2011; Nguyen, Bedford, Bretana, & Hayes, 2011; Oulasvirta, Pihlajamaa, Perkiö, Ray, Vähäkangas, Hasu, & Myllymäki, 2012).

The amount as well as the scope and type of data a smart speaker collects, worries consumers (Fruchter & Liccardi, 2018; Pridmore et al., 2019). Various recent scandals, such as Amazon's Echo mailing of a private dialog to an owners' address contract, increase owner's and potential owner's privacy concerns (Pridmore et al., 2019).

As Chhetri and Mottie (2019) state in their study, the top user privacy concerns are: always listening to conversations, user tracking, storage of data in the cloud, data security, hacking of data and sharing (public/third-party/government). Users are mostly concerned that microphones installed in smart speakers record private conversations (Pridmore et al., 2019) as well as background conversations and noises which were not directed to the device (Chhetri & Motti 2019; Lau et al., 2018). Those concerns can lead to a decreased willingness to share private data with the device. This, in turn, may result in negative attitudes towards smart speakers.

(H2): High privacy concerns negatively affect the attitude towards smart speakers

2.3.4. Trust in the service provider

Trust is a central factor which has been broadly researched in many areas of academic literature before. Due to its adaptability and broadness, many definitions of trust coexist. While Luhmann (1976) defines trust as the belief by one party about another party that the other party will behave in a predictable manner, Mayer, Davis, and Schoorman (1995) state that trust can be defined as: "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (p. 712).

Besides, trust is usually classified in the three dimensions benevolence, integrity, and competence. These dimensions define the trustworthiness of the involved parties. When purchasing products online, consumers often rely on trust. Thereby, technology, which is typically the organizations' website, or in this case the IoT device, is the object of trust (Beldad, De Jong, & Steehouder, 2010). Online trust can be characterized as "a reliance on a firm by its stakeholders with regard to its business activities in the electronic medium" (Corritore, Kracher, & Wiedenbeck, 2013, p. 325).

Trust is widely known for influencing privacy risks and attitude of IoT users (Worthy et al., 2016; Zheng et al., 2018). Many owners of smart speakers distrust their device (Fruchter

& Liccardi, 2018) but research found that famous companies like Google or Amazon are normally trusted by consumers (Pridmore et al., 2019). Lau et al. (2018) highlight that it is in the best interest of companies to protect their customers. Additionally, the GDPR, the regulation in EU law on data protection and privacy, which came into effect in 2016, increased internet and online consumers' trust (Sharma & Crossler, 2014).

Nevertheless, certain reports in the media lately claim that commonly used smart speakers such as Alexa or Google Home are not always trustworthy (Chung, Iorga, Voss, & Sangjin, 2017; Pridmore et al., 2019; Zeng, Mare, & Roesner, 2017). Especially retailers of devices which collect personal data such as smart speakers depend on trust from their customers since consumer trust may mitigate privacy concerns (Bleier & Eisenbeiss, 2015). In the study of Moloney and Poti (2013), trust was already incorporated in the privacy calculus model. Adding trust as a variable means that a dispositional factor complements the more rational process of privacy calculus. Additionally, trust has been examined in the context of the TAM before (Beldad & Hegner, 2017). In the present study, all three types of trust are considered under the general term "trust". Thus, it is assumed that:

(H3): High trust in the service provider positively affects the attitude towards smart speakers

2.3.5. Intrusive technology features

According to Ayyagari, Grover, & Purvis (2011), intrusive technology is characterized as information technologies' invasiveness and describes a component of the person technology fit model which predicts individuals' stress as an outcome of technology use (Edwards, Cable, Williamson, Lambert, & Shipp, 2006). The most common features in this field are technology presenteeism and anonymity. However, a call for further investigation into different context related features has been made (Ayyagari et al., 2011; Benlian, et al., 2019).

In their research, Benlian et al. (2019) responded to this call and investigated the role of unintentional voice activation of smart home assistants and the effect on individual strain. They found that unintentional voice activations lead to a misfit between users' need for privacy and the demand for a digitized environment. The perceived benefits of smart speakers decrease when the device is activated unintentionally (Benlian et al., 2019). Relating the findings to the context of this study, it can be stated that unintentional voice activation negatively influences perceived usefulness since an unintentionally activation of the smart speaker disturbs the convenience of the device. Unintentional voice activations are among the most mentioned privacy-invasive issues of consumers (Chhetrie & Mottie, 2019; Lau et al., 2018). They are considered privacy intervention and can lead to privacy concerns (Ayyagari, 2011). When a smart speaker is activated unintentionally, private conversation can be recorded accidentally

and send to the cloud. More specifically this means that unauthorized parties such as commercial parties or hackers can access the data which was originally not supposed to get recorded by the smart speaker nor saved in the cloud. For this reason, unintentional voice activations prove that users do not have full control over their voice data (Chung et al., 2017; Ford & Palmer, 2019).

Another feature of smart speakers that individuals find highly intrusive is that the recordings are listened to and evaluated by real humans. For example, employees of Amazon are "tasked with transcribing users' commands, comparing the recordings to Alexa's automated transcript, say, or annotating the interaction between user and machine" (Day et al., 2019). Consumers perceive machines to be more trustworthy than humans when it comes to data processing (Ray, 2019; Winder, 2019). People's attitude towards data evaluation by humans (vs. data collection by machines or software) has been researched in the context of smart speakers before by Malkin et al. (2019). The authors asked participants in a study whether they preferred their speech data be analyzed by a machine or a human being for the purpose of quality control. The results show that computer reviews are considered more acceptable than human data evaluation. These outcomes are in line with an article by Hurtz (2019) who claims that data evaluation by humans leads to an increase of privacy concerns and decreases trust in the service provider. He argues that most users are convinced that only machines analyze voice data of smart speakers, which results in terrified reactions when consumers experience the opposite. The author empathizes his arguments with examples of privacy incidents with smart speakers which were published in media.

In contrast to this, we expect that data evaluation by humans as an intrusive feature will positively influence perceived usefulness since non-owners might expect that the data analysis from employees (compared to machines) result in better quality improvements of the devices even if they prefer analysis by software in terms of privacy.

Chhetri and Motti (2019) refer the influence of intrusive features on the attitude towards smart speakers but do specifically analyze it. Overall, the effect of intrusive features on the attitude towards smart speakers does not frequently appear in literature about privacy of IoT devices. Further exploration into the effect of specific features on the attitude towards smart speakers is needed referring to the call for further investigation into different context-related intrusive features by Ayyagari et al. (2011). With regard to the present study, it is assumed that intrusive features like unintentional voice activation and data evaluation by humans have a direct, negative effect on the attitude towards smart speakers. Thus, the attitude is assumed to be lower when those features are present. Therefore, the following two hypotheses are assumed:

(H4): The attitude towards smart speakers is higher when voice activation is intentional (compared to unintentional).
(H5): The attitude towards smart speakers is higher when the data is evaluated by software (compared to humans).

Additionally, intrusive features also strike at the core of privacy concerns, perceived benefits, and trust in a way mentioned above and are of high theoretical relevance for this study. Thus, following hypotheses are assumed:

(H6): Perceived usefulness is higher when the smart speaker is activated intentionally (compared to unintentionally) by voice.
(H7): Perceived usefulness is higher when the data on the smart speaker is evaluated by humans (compared to software).
(H8): Privacy concerns are higher when the smart speaker is activated unintentionally (compared to intentionally) by voice.
(H9): Privacy concerns are higher when the data on the smart speaker is evaluated by humans (compared to software).
(H10): Trust in the service provider is higher when the smart speaker is activated intentionally (compared to unintentionally) by voice.
(H11): Trust in the service provider is higher when the data on the smart speaker is evaluated by software (compared to humans).

2.3.6. Interaction effects

Besides the main effects, several interaction effects of the two intrusive features are possible. We assume two interaction effects, based on the arguments and hypotheses described above. First, two intrusive features are assumed to lead to higher privacy concerns than one intrusive feature. Therefore, the following hypothesis is formulated:

(H12): When the data is evaluated by humans (compared to software), privacy concerns are higher when the smart speaker is activated unintentionally than intentionally.

Second, as explained above, trust is expected to be lower when the smart speaker is activated unintentionally. Consequently, trust is higher when the smart speaker is activated intentionally. When the intrusive feature (unintentional voice activation) is not present and instead the smart speaker is activated intentionally, it is assumed that data evaluation by humans leads to higher trust (compared to data evaluation by software). Despite contradicting previous research

(Malkin et al., 2019), it is supposed that data evaluation by software is less trusted by non-owners but only if the smart speaker is activated intentionally because it might be possible that consumers distrust big data analytics even more than evaluation by humans.

(H13): Trust in the service provider is higher when the data is evaluated by humans than by software when the smart speaker is activated intentionally (compared to unintentionally).

2.3.7. The mediating roles of perceived usefulness, privacy concerns, and trust

As presented above, direct effects of perceived usefulness, privacy concerns, and trust on the dependent variable attitude towards smart speakers are assumed. Additionally, Ayyagari et al. (2011) claim that privacy technology features influence the attitude towards a device. In the present study, it is assumed that this effect is mediated by perceived usefulness, privacy concerns, and trust. Referring to voice activation, authors state that unintentional voice activation decreases perceived usefulness, and trust (Hurtz, 2019) and increases privacy concerns (Benlian et al., 2019; Chhetrie & Mottie, 2019; Lau et al., 2018) which are, in turn, generally perceived as influencing attitude towards smart speakers (Fruchter & Liccardi, 2018; Pridmore et al., 2019).

In the other case of data evaluation, Malkin et al. (2019) provide evidence for the fact that users' acceptance of smart speakers decreases with the knowledge that their personal voice data could be analyzed by employees. This study investigates whether this effect also applies to the attitude of potential consumers and whether the variables privacy concerns and trust act as mediators on this effect. In addition, it is supposed that perceived usefulness mediates the effect of data evaluation on attitude. Therefore, the following hypotheses are proposed:

(H14a): Perceived usefulness mediates the effect of voice activation on the attitude towards smart speakers.
(H14b): Perceived usefulness mediates the effect of data evaluation on the attitude towards smart speakers.
(H15a): Privacy concerns mediate the effect of voice activation on the attitude towards smart speakers.
(H15b): Privacy concerns mediate the effect of data evaluation on the attitude towards smart speakers.
(H16a): Trust in the service provider mediates the effect of voice activation on the attitude towards smart speakers.

(H16b): Trust in the service provider mediates the effect of data evaluation on the attitude towards smart speakers.

2.4. Conceptual model

Several hypotheses were formed based on the literature mentioned in the theoretical framework. An overview of the hypotheses can be found in Table 1.

Table 1
List of hypotheses

	Hypothesis
H1	High perceived usefulness positively affects the attitude towards smart speakers.
H2	High privacy concerns negatively affect the attitude towards smart speakers.
H3	High trust in the service provider positively affects the attitude towards smart speakers.
H4	The attitude towards smart speakers is higher when voice activation is intentional (compared to unintentional).
H5	The attitude towards smart speakers is higher when the data is evaluated by software (compared to humans).
H6	Perceived usefulness is higher when the smart speaker is activated intentionally (compared to unintentionally) by voice.
H7	Perceived usefulness is higher when the data on the smart speaker is evaluated by humans (compared to software).
H8	Privacy concerns are higher when the smart speaker is activated unintentionally (compared to intentionally) by voice.
H9	Privacy concerns are higher when the data on the smart speaker is evaluated by humans (compared to software).
H10	Trust in the service provider is higher when the smart speaker is activated intentionally (compared to unintentionally) by voice.
H11	Trust in the service provider is higher when the data on the smart speaker is evaluated by software (compared to humans).
H12	When data evaluation is done by humans (compared to software), privacy concerns are higher when the smart speaker is activated unintentionally than intentionally.
H13	Trust in the service provider is higher when the data is evaluated by humans than by software when the smart speaker is activated intentionally (compared to unintentionally).
H14a	Perceived usefulness mediates the effect of voice activation on the attitude towards smart speakers.
H14b	Perceived usefulness mediates the effect of data evaluation on the attitude towards smart speakers.
H15a	Privacy concerns mediate the effect of voice activation on the attitude towards smart speakers.
H15b	Privacy concerns mediate the effect of data evaluation on the attitude towards smart speakers.

H16a	Trust in the service provider mediates the effect of voice activation on the attitude towards smart speakers.
H16b	Trust in the service provider mediates the effect of data evaluation on the attitude towards smart speakers.

To answer the three research questions: Q1: *How do perceived usefulness, privacy concerns, and trust influence the attitude towards smart speakers of non-owners?; Q2: To what extent do voice activation and data evaluation influence the attitude of potential smart speaker owners?; Q3: To what extent is the effect of voice activation and data evaluation on attitude towards smart speakers mediated by perceived usefulness, privacy concerns, and trust?,* we propose a comprehensive model (Figure 1) which tests all the above-mentioned hypotheses.

This model includes two independent variables (voice activation and data evaluation), one dependent variable (attitude towards smart speakers) and three mediation variables (perceived usefulness, privacy concerns, and trust), which influence the effects between the two independent variables and the depend variable. Additionally, the variables perceived usefulness, privacy concerns, and trust have a main effect on attitude towards smart speakers. Furthermore, two interaction effects are assumed.

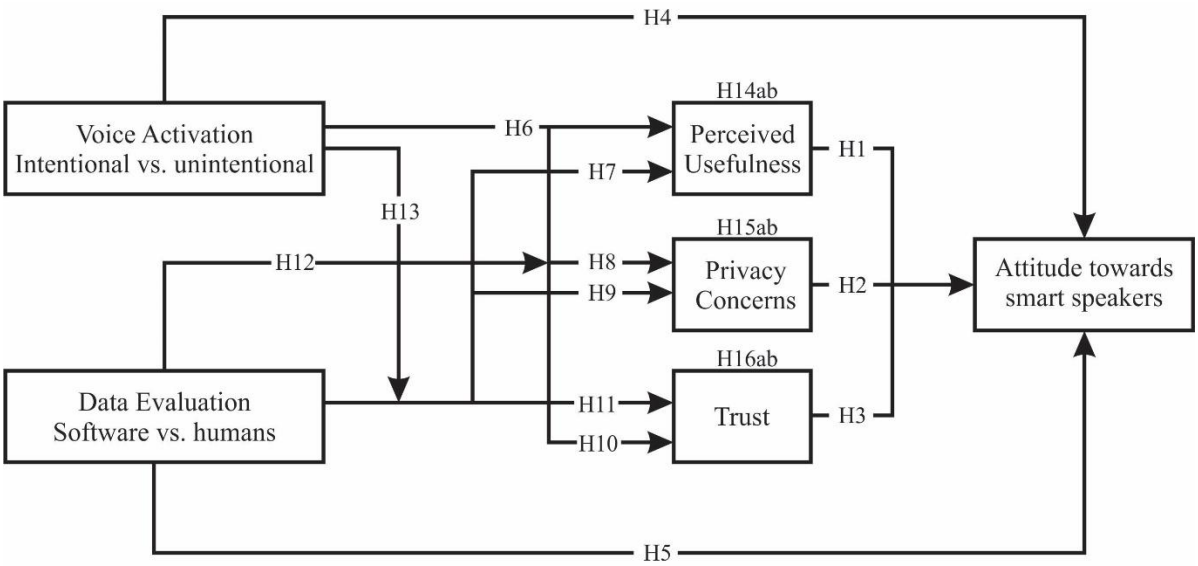


Figure 1
Conceptual Model

3. Method

3.1. Research Design

As a method for this research, a 2x2 between-subject online experiment was conducted in which two independent variables (voice activation and data evaluation) were manipulated resulting in four conditions. The experimental conditions can be found in Table 2.

The causal research technique included a vignette scenario. Although vignette scenarios have downsides such as simplification, they offer the advantage of controlling participants' experience and avoiding socially desirable bias (Aguinis & Bradley, 2014). Furthermore, they offer to apply precise manipulations, scrutinize the impact on dependent variables and identifying interaction effects (Benlian et al., 2019) and have been applied successfully in previous studies on privacy (Weidman, Aurite, & Grossklags, 2019) and intrusive technology features (Benlian et al., 2019. This demonstrates that this technique is valid and effective in measuring attitudes and concerns to context-related privacy issues of smart speakers.

The independent variables (unintentional vs. intentional voice activation and data evaluation by humans vs. by software) were manipulated by the vignette scenarios to test the effect on the dependent variable (attitude towards smart speakers) by means of a questionnaire. Additionally, the effect of mediation variables (perceived usefulness, privacy concerns, and trust) on attitude were tested.

Table 2
Experimental conditions

Conditions	Voice activation	Data evaluation
Condition 1 (N=52)	Unintentional	Software
Condition 2 (N=39)	Unintentional	Humans
Condition 3 (N=50)	Intentional	Software
Condition 4 (N=45)	Intentional	Humans

3.2. Stimuli Design

Pre-test

A pre-test was conducted before doing the main study, to verify the validity of the stimulus materials. The pre-test aimed to determine if the vignette scenario was clearly formulated, realistic and understandable for participants, regarding the (un)intentional voice activation and the data evaluation by humans (vs. software). The goal of the focus group was to unite on one vignette scenario with voice activation and on another one with data evaluation. Additionally, it was important to determine which kind of voice activation was perceived as intrusive.

As a technique, an (online) focus group was chosen. Focus groups as a technique of qualitative research are known for improving the measurement validity of experiments and surveys by ensuring that the material is properly contextualized and that the manipulations work as intended. During focus groups, a small group of people openly discuss a topic in the presence of a moderator. Thereby, the group shares their feedback and opinions (Cyr, 2019).

The focus group in the present study consists of 8 participants between the age of 22 and 26, five female and three been male. All participants are German; therefore, the focus group was held in German and the vignette scenarios were prepared in German as well. The group was asked to share comments on five different vignette scenarios (three involving voice activation and two involving data evaluation). All scenarios described a fictional dinner date of two friends in the presence of a recently adopted smart speaker called Nozama. The fictious smart speaker brand (Nozama) was chosen to avoid bias by present opinions and preferences on known brands.

Most of the participants perceived the unintentional voice activation in all versions as intrusive. However, the first example that was shown was rated as less intrusive than the other two. The example with the personal conversation about a divorce was rated as most intrusive but also as not easy to understand as one participant said: “Wow, that is highly intrusive but it seems not really natural and hard to comprehend why the smart speaker gets activated by itself.” The third version including the unintentional activation of music was perceived as intrusive and understandable. Therefore, this version was chosen for the main study.

Regarding data evaluation, participants suggested to combine both versions (textual and visual material) for the article about data processing of smart speakers because they preferred the pictures of the second version but considered the textual description highly important for understanding. One participant said: “The pictures help in understanding, but the text also underlines the intrusiveness of data processing, I would think about combining them”. After the focus group, the feedback was evaluated and the vignette scenarios were adjusted.

As a result, the third (un)intentional voice activation scenario (with some change in wordings) and a combination of both data evaluation scenarios (text and pictures) was chosen for the main study. The participants of the pre-test did not take part in the finale online experiment. The scenarios used for the pre-test can be found in the Appendix (A).

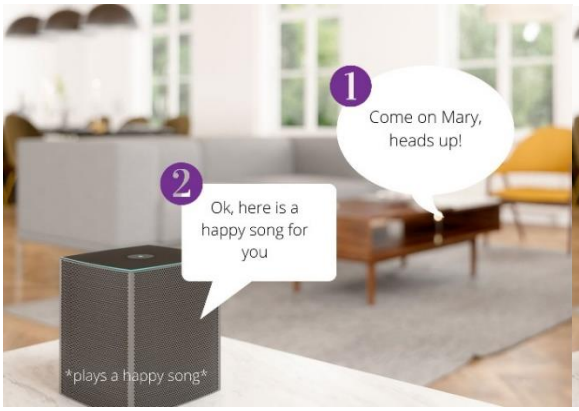
Main study

The main study comprises four conditions with each condition instructing participants to slip into the role of Tom. It aims to manipulate participants through either showing an intrusive feature of smart speakers or not. In the vignette scenario, Tom was invited by his friend Mary for dinner who recently purchased a new smart speaker. Participants were provided with the background information that the smart speaker is usually activated with the wake word:

“Nozama”. The variable *voice activation* was manipulated by showing participants a scenario with unintentional or intentional voice activation. In the *intentional voice activation* condition, Alex activates the smart speaker intentionally by saying *“Nozama play some happy songs”*. In the *unintentional voice activation* condition Alex activates the smart speaker unintentionally with the wording *“Come on Mary, heads up”*. In both situations, the smart speaker starts playing a song, i.e. gets activated.

Then, the scenario continues with Alex going home and reading a short notification about the data evaluation process of smart speakers. Thereby, the variable *data evaluation* was manipulated by presenting a situation with data evaluation by software or by humans. In the *data evaluation by software* condition, he learns that the voice data is evaluated by software through reading a statement from a data protection specialist. In the condition with *data evaluation by humans* the same statement is provided but this time it states that voice data is evaluated by humans. All textual descriptions of the scenarios were adjusted with a visual description which included the manipulations (unintentional vs. intentional voice activation x data evaluation by software vs. by humans). Through this, the intrusive features of smart speakers were more tangible and understandable for the participants. The scenario can be found in Appendix B. The visual manipulations are demonstrated in Figure 2.

Unintentional voice activation



Intentional voice activation

Data evaluation by software

Date evaluation by humans

Figure 2
Visual manipulations

3.3. Measurement

Measurement scales were adopted from previous studies which established their validity and reliability. If necessary, they were adapted to fit in the context of smart speakers. Some measurement scales were self-generated. Items of the conceptual model were tested by a 7-point Likert scale from 1 (strongly disagree) till 7 (strongly agree). The entire questionnaire is listed in Appendix B and the measurement scales are in Appendix C.

Perceived usefulness was measured by scales from Princi and Krämer (2020), adjusted with scales from Yang and Lee (2019). As explained above, several terms which symbolize specific benefits were summarized under the term perceived usefulness. One example of these scale items which relates to convenience is: “Using a smart speaker would give me convenience at home”. Another one which relates to enjoyment is: “Using a smart speaker would give me pleasure” and one which relates to personalization is: “It is great that smart speakers are customized to my personal needs”. “Using a smart speaker would make my everyday life easier”, relates to perceived usefulness. In total, *perceived usefulness* was measured through five items.

Privacy concerns were measured using scales from Kowalsczuk (2018) and Yang, Lee, and Zo (2017) as well one self-generated scale. In total, five items were used for measuring *privacy concerns*. One example question is: “It is risky to disclose private information to a smart speaker”. Another one was “I am concerned that smart speakers would track my private information.“ Trust was measured using five items from Yang et al. (2017) such as “I think smart speaker service providers are reliable” or “I perceive smart speaker providers as trustworthy”.

Attitude was measured twice because on one hand, general attitudes towards smart speakers were of interest and on the other hand, specific attitudes towards the smart speaker in the manipulated scenario (Nozama) should be measured. Using scales from Fortes et al. (2017) and some self-generated scales, five items were created measuring *attitude towards Nozama* (as a fictional- example for one specific smart speaker). For instance, “I have positive feelings towards Nozama” or “My attitude towards Nozama is positive” were two of the items. Attitude was measured a second time, measuring a more general attitude towards smart speakers. Thus, the item *attitude towards smart speakers* was measured using the same scale but replacing Nozama through smart speakers.

Additionally, to test whether the vignette scenario correctly manipulated participants, a manipulation check was done. The manipulation check was carried out at the very end of the survey questionnaire. For each of the two manipulations one question was asked. More specifically, to check whether the voice activation scenario was successful, participants were asked whether Tom activated the smart speaker with the activation word “Nozama” or not. The manipulation of the second scenario was tested by asking whether the article claimed that the evaluation of the voice data was carried out by software or humans.

To ensure the validity and reliability of the measurements, most of the scales in the follow-up survey were adopted from existing literature. These constructs have already been used for studies about privacy and IoT. In this way, the validity and reliability were already proven. Only some reformulations had to be made to adjust them for the special case of smart speakers and some few constructs were self-generated. As mentioned before, the statements in the questionnaire were answered on a 7-point Likert scale which provides a broad variety of answer options. In conclusion, it "provides more varieties of options which in turn increase the probability of meeting the objective reality of people" (Joshi, Kale, Chandel, & Pal, 2015, p. 398).

A factor analysis was conducted to test whether all the items loaded in the right constructs and to test the validity of the questionnaire. When running the first factor analysis, the items of the five constructs (attitude towards Nozama, perceived usefulness, privacy concerns, trust, and attitude towards smart speakers) resulted in four constructs. Thus, not all items loaded in the scales as proposed. The items of attitude towards smart speakers loaded in the construct of attitude towards Nozama and perceived usefulness. As a solution, the five items (of attitude towards smart speakers) that loaded in both constructs were deleted, leaving attitude towards Nozama as an independent variable for the model. The items of perceived usefulness which included several terms all loaded as proposed in one factor. Consequently, the factor analysis resulted in four constructs with 20 items in total. All remaining items loaded a value higher than .50. To ensure reliability, Cronbach's alpha was calculated for all constructs. A minimum value of .70 is needed to consider a construct as reliable. The lowest measured construct shows an alpha value of .88 and the highest .90. Thus, all constructs can be categorized as highly reliable. The reliability and the factor analysis can be found in Table 3 below.

Table 3
Reliability and factor analysis

Construct	Item	1	2	3	4
Perceived usefulness .90	Using a smart speaker would give me convenience at home	.86			
	Using a smart speaker would give me pleasure	.77			
	I find smart speakers convenient in day-to-day life	.85			
	Using a smart speaker would make my everyday life easier	.84			
	It is great that smart speakers are customized to my personal needs	.67			
Trust .88	I think smart speaker service providers are reliable		.79		
	I perceive smart speaker providers as trustworthy		.77		
	I think smart speaker providers like keep customers' best interests in mind		.68		
	I believe smart speaker service providers to be honest		.80		
	I think smart speaker service providers keep promises and commitments		.80		
Privacy Concerns .89	It is risky to disclose private information to a smart speaker			.69	
	I am worried that smart speaker will store my private data			.72	
	My private information on a smart speaker could be misused			.86	
	Companies would collect too much personal information about me if I would use a smart speaker			.77	
	I am concerned that smart speakers would track my private information			.83	
Attitude towards Nozama .89	I have positive feelings about Nozama				.77
	Nozama is a great invention				.74
	I really like Nozama				.73
	My attitude towards Nozama is positive				.73
	I am really interested in Nozama				.55

3.4. Procedure

The main study was distributed online via a link. Before the experiment and the questionnaire started, participants were asked for consent. In the first part of the experiment, demographic information of the participants was queried, as well as their familiarity with and personal opinions about smart speakers. For the possible case, that some participants might not be familiar with smart speakers, participants were provided with a short information text about smart speakers before they started with the second part of the questionnaire. The second part contained the 2x2 between-subjects experiment described above to test the proposed model. Participants only saw one of four conditions to which they were randomly assigned to. Afterwards, they were asked to fill out the questionnaire with the scales to measure attitude, perceived usefulness, privacy concerns, and trust.

The questionnaire was originally created in English and translated to German to reach a larger sample. For validity reasons, the questionnaire was translated back from German to English by a certified translator. Participants had the option to set the language to German or English.

3.5. Participants

Participants for the experiment were scouted through the personal network of the researcher and recruited using snowball sampling. Thus, the questionnaire was spread online via social media channels like Facebook, LinkedIn, and WhatsApp. Participants were asked as a second step to further forward the link to their network to reach as many participants as possible. They participated voluntarily and did not receive a compensation.

The desired number of participants was 120 to get reliable results because we were aiming for at least 30 participants for each condition (4x30=120). Participants were evenly and randomly assigned to the conditions. The total number of collected answers was 307. From this number, 44 participants said they already own a smart speaker. Since the study aimed to consist of participants who do not own a smart speaker, those 44 respondents were not considered for the analysis. Another number of 77 participants were filtered out by the control questions at the end of the survey. Thus, a total number of 186 questionnaires were used for the data analysis. The mean age of the total sample was 29.28 (sd=10.8). 119 (64%) answers were from female and 67 (36%) from male participants.

More than 95 % of respondents knew what a smart speaker was, while around half of participants had already used the device. Remarkably, more than 80 % of individuals did not consider buying a smart speaker, 10 % did not know yet and only 8% had the intention to buy a smart speaker in the future. Participants of the experimental study also indicated their nationality, 159 were German (85,5%) and 15 Dutch (8,1%), the remaining 12 (6,5%) had another nationality. Table 4 below shows the demographic information across the different conditions.

Table 4
Demographics of the four conditions

Condition	N	Age	Gender (%)	
		Mean (SD)	M (%)	F (%)
1	52	29.94 (12.1)	20 (38.5)	32 (61.5)
2	39	27.90 (7.6)	14 (35.9)	25 (64.1)
3	50	28.68 (10.4)	19 (38)	31 (62)
4	45	30.40 (12.1)	14 (31.1)	31 (68.9)
Total	**186**	**29 (10.8)**	**67 (36)**	**119 (64)**

Conditions:
Condition 1: *Unintentional voice activation x data evaluation by software*
Condition 2: *Unintentional voice activation x data evaluation by humans*
Condition 3: *Intentional voice activation x data evaluation by software*
Condition 4: *Intentional voice activation x data evaluation by humans*

3.6. Analysis

To analyse the data and the proposed model, the statistical analysis program SPSS was used. Constructs were grouped into scales and the four different conditions were transformed into two variables (voice activation and data evaluation).

A multivariate analysis of variance (MANOVA) was used to examine the effect of voice activation and data evaluation on the dependent/intervening variables. Before the analysis took place, it was investigated if the six underlying assumptions of MANOVA were met. The criteria of independence and cell size were met since each participant only participated once in the study and the number of cases was greater than the number of independent variables. The univariate normality assumption was violated because of a series of significant Shapiro-Wilk tests. Additionally, the Mahalanobis distance analysis found some outliers in the data, violating the assumption of multivariate normality. Because MANOVA is quite robust against normality violations when group size exceeds 30 participants (Allen & Bennet, 2012) we decided to continue with the analyses. Correlation between the dependent variables were not excessive which indicates that multicollinearity was not of concern. Finally, Box's M was non-significant at alpha (*a*.=.001).

4. Results

The main goal of this research was to investigate the effects of voice activation and data evaluation on attitude as well as on perceived usefulness, privacy concerns, and trust. This chapter presents the interpretation and analysis of the results. First, the main effects of perceived usefulness, privacy concerns, and trust on attitude towards Nozama are presented via a regression analysis. Thereby, the four conditions are combined since voice activation and data evaluation are not part of this analysis. Second, the main effects of voice activation and data evaluation on the dependent variables are introduced. Afterwards, interaction and mediation results will be demonstrated.

4.1. Main effects of perceived usefulness, privacy concerns, and trust

In Table 5, both mean scores and standard deviations of the measured constructs in the questionnaire on a 7-point Likert scale are shown. The results demonstrate how non-users perceive smart speakers in terms of attitude, trust, usefulness, and privacy concerns. With 6.24 privacy concerns had a very high mean score. Attitude had the lowest mean score, while trust was also low and perceived usefulness rather low.

Table 5
Descriptive Statistics

Variable	Frequency (N)	Mean	SD
Attitude	186	2.51	1.21
Perceived Usefulness	186	3.59	1.48
Privacy Concerns	186	6.24	0.83
Trust	186	2.77	1.13

Note:
Variables measured on a 7-point Likert scale (1=strongly disagree – 7=strongly agree)

A regression analysis was conducted to test the relationship of perceived usefulness, privacy concerns, trust, and attitude. Before, the constructs were tested for correlation. Table 6 shows Pearson's correlation for the different variables. The strongest positive correlation is between attitude and perceived usefulness ($r=.62$, $p<.01$) and the strongest negative correlation between privacy concerns and attitude ($r=-.61$, $p<.01$). Additionally, strong correlation can be found between trust and attitude ($r=.57$, $p<.01$) and a strong negative correlation between trust and privacy concerns ($r=-.49$, $p<.01$). Furthermore, moderate correlations are between

perceived usefulness and privacy concerns (r=-.34, p<.01) and between perceived usefulness and trust (r=.36, p<.01).

Table 6
Correlation between constructs

	A	PU	PU	T
Attitude	1			
Perceived Usefulness	.62**	1		
Privacy Concerns	-.61**	-.34**	1	
Trust	.57**	.36**	-.49**	1

**. Correlation is significant at the 0.01 level (2-tailed)

In Table 7, a multiple linear regression analysis was conducted to test the first three hypotheses. H1 was supported. Through linear regression the effect of perceived usefulness on attitude was tested. The outcome of the multiple regression analysis showed that the effect of perceived usefulness as an independent variable and attitude towards Nozama as a dependent variable was significant (β = .41; t (186) = 8.09; p < .001). This means that perceived usefulness is a significant positive predictor of attitude towards Nozama. The higher potential consumers perceive the usefulness of smart speakers, the higher is their attitude towards Nozama.

H2 was also supported. The results of the linear regression analysis showed that the effect of privacy concerns on attitude was significant (β = -.51; t (186) = -6.47; p < .001). This result revealed that high privacy concerns lead to a more negative attitude towards Nozama. This means that privacy concerns are a negative predictor of attitude.

H3 was supported. Linear regression was used to predict the effect of trust on attitude. The regression was found to be significant (β = .26; t (186) = 4.48; p < .001). Therefore, high trust positively effects the attitude towards Nozama.

Table 7
Multiple regression analysis for attitude towards Nozama

Variable	B	SE	β	t	p
Perceived Usefulness	.33	.04	.41	8.09	.000
Privacy Concerns	-.51	.08	-.34	-6.47	.000
Trust	.26	.06	.25	4.48	.000

Note:
R^2 =.607

4.2. Main effects of intrusive technology features

To investigate the effect of intrusive technology features (unintentional voice activation and data evaluation by humans) on the (mediating/depending) variables perceived usefulness, trust, privacy concerns, and attitude towards Nozama a multivariate analysis of variance (MANOVA) was conducted. Table 8 shows the outcome of the MANOVA test. A Wilks' Lambda was conducted to examine the different effects of the independent variables. As Wilks' Lambda's show, no significant main effects of voice activation (Λ = .99, F = 0.63, p = .64) and data evaluation (Λ = .977, F = 1.08, p = .37) on the combined dependent variables were shown. Furthermore, there were also no significant results for the interaction effect of voice activation and data evaluation on the combined dependent variables (Λ = .97, F = 1.37, p = .25).

Table 8
Outcome of the multivariate test of independent variables

	Wilks' Lambda	F-Value	Sign.
Voice activation	.99	.63	.64
Data evaluation	.98	1.08	.37
Voice activation*data evaluation	.97	1.37	.25

Note:
Significant at *a*.=.05

Additionally, table 9 below shows the outcome of the between-subject experiment. The table shows the significant effects at alpha (*a*.=.05) across the different variables.

Table 9
Test of between-subject outcomes of independent on dependent variables

	Dependent Variable	F-Value (1,182)	Sign.
Voice activation	Perceived Usefulness	.55	.46
	Trust	.01	.93
	Privacy Concerns	.19	.66
	Attitude Nozama	.81	.18
Data evaluation	Perceived Usefulness	**3.16**	**.08**
	Trust	1.72	.19
	Privacy Concerns	.32	.57
	Attitude Nozama	.60	.44
Voice activation*data evaluation	Perceived Usefulness	.33	.57
	Trust	**3.53**	**.06**
	Privacy Concerns	1.01	.32
	Attitude Nozama	.61	.44

Note:
Significant at *a*.=.05
All dependent variables measured on a 7-point Likert scale (1=strongly disagree – 7=strongly agree)

H4 stated that the attitude towards smart speakers would be higher if voice activation was intentional (compared to unintentional). As can be seen in Table 9, this effect was not supported since the difference was not significant (F(1, 182)=1.81, p=.18). H5 was also not supported. The type of data evaluation has no significant effect (F(1, 182)=.60, p=.44) on the attitude towards Nozama. H6 was also not supported. Table 9 does not show a significant effect (F(1, 182)=.55, p=.46) for voice activation on perceived usefulness.

However, there is a marginally significant effect of data evaluation on perceived usefulness (F(1, 182)=3.16, p=.08). Perceived usefulness is higher when data evaluation is done by humans (M=3.42, SD=1.57) compared to software (M=3.81, SD=1.35). Consequently, Hypothesis 7 is partially supported.

H8 and H9 were not supported since the difference in means for privacy concerns were not significant for both H8 (F(1, 182)=.19, p=0.66) and H9 (F(1, 182)=.32, p=.57). Also, the difference in means for trust were not significant either for the type of voice activation (F(1, 186)=.01, p=.93), nor for the type of data evaluation (F(1, 186)=1.72, p=.19). Therefore, H10 and H11 were not supported. Table 10 shows the mean scores for the effect of voice activation and data evaluation on attitude.

Table 10
Descriptives of independent on the dependent variables

		Mean (SD)			
Voice Activation	Data Evaluation	Perceived usefulness	Trust	Privacy Concerns	Attitude
Unintentional	Software	3.28 (1.63)	2.81 (1.15)	6.24 (0.92)	2.40 (1.29)
	Humans	3.79 (1.48)	2.72 (1.13)	6.10 (0.70)	2.39 (1.17)
	Total	3.50 (1.58)	2.77 (1.14)	6.26 (0.83)	2.40 (1.18)
Intentional	Software	3.56 (1.51)	2.52 (0.96)	6.31 (0.73)	2.50 (1.18)
	Humans	3.83 (1.25)	3.04 (1.24)	6.12 (0.92)	2.78 (1.27)
	Total	3.69 (1.39)	2.77 (1.13)	6.22 (0.83)	2.63 (1.22)
Total	Software	3.42 (1.57)	2.67 (1.07)	6.27 (0.32)	2.45 (1.19)
	Humans	3.81 (1.35)	2.89 (1.19)	6.20 (0.83)	2.60 (1.23)
	Total	3.59 (1.48)	2.77 (1.13)	6.24 (0.83)	2.51 (1.21)

4.3. Interaction effects

H12 was rejected since the interaction effect between voice activation and data evaluation on privacy concerns was not significant (F(1, 182)=1.01, p=.32). Interestingly, results in Table 9 indicated that there is a marginally significant interaction effect between the two variables voice activation and data evaluation on trust (F(1, 182)=3.53, p=.06). The plot of this interaction is shown in Figure 3. It shows that in the case of unintentional voice activation, participant's trust

in the smart speaker service provider is approximately the same for either data evaluation by software (*M*=2.81, *SD*=1.15) or by humans (*M*=2.72, *SD*=1.13). However, in the conditions with intentional voice activation participants' trust was marginally lower when data evaluation was done by software (*M*=2.52, *SD*=0.96) than by humans (*M*=3.04, *SD*=1.24). This means that trust in the smart speaker service provider is highest when voice activation is intentional and data evaluation is done by humans. Consequently, H13 was partially supported.

Additionally, a moderated mediation analysis was conducted using the process test of Andrew F. Hayes through model 7. The test was used to check if trust meditates the interaction between voice activation and data evaluation on attitude. The result of analysis showed that voice activation (*b*=.918, *p*=.073) does not significantly predict trust. Instead, the effect is only marginally significant. Data evaluation (*b*=.716, *p*=.177) also does not significantly predict trust since p>.05. The result also reveals that voice activation (*b*=-.235, *p*=.108) does not significantly predict attitude, but trust (*b*=.605, *p*=.000) does significantly predict attitude since *p*<.05.

According to the result, the interaction of voice activation and data evaluation also did not significantly effect attitude since *p*=.4741>.05 and *F*(1,182)=.5145.

Furthermore, the analysis of Hayes stated that if the null of H0 does not fall between the lower and upper limit of the 95% confidence interval, the moderation mediation hypothesis is supported. In the present outcome, the confidence interval does include zero (95% CI: -.787 to .027), thus moderated mediation is not established.

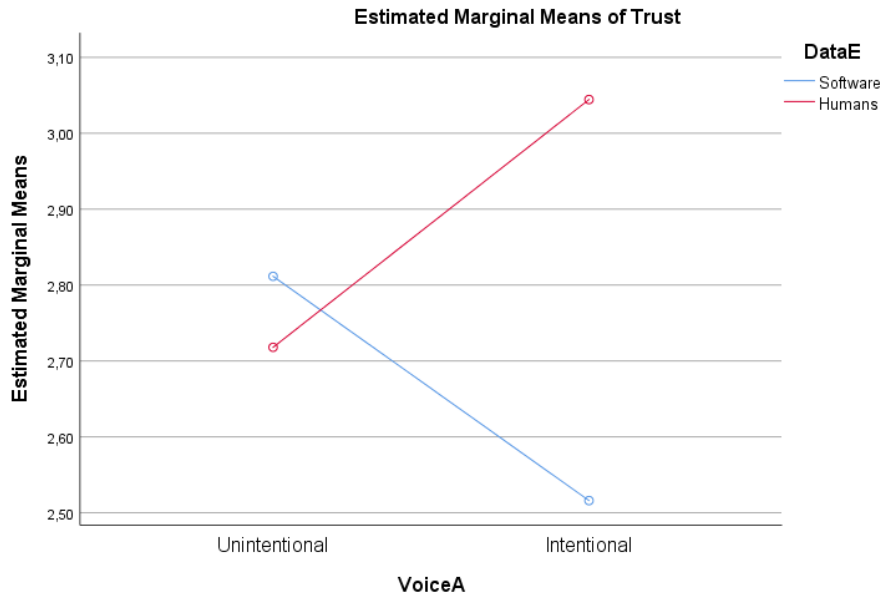


Figure 3
Interaction effect of voice activation and data evaluation on trust

4.4. Mediation effects

The mediation effects of perceived usefulness, privacy concerns, and trust were tested using process of Andrew F. Hayes model 4.

Perceived usefulness

In Step 1 of the mediation model, the regression of voice activation on attitude towards Nozama, ignoring the mediator (perceived usefulness), was not significant, b = -.232, $t(186)$ = -1.313, p = .191. Next, Step 2 showed that the regression of voice activation on the mediator, perceived usefulness, was not significant, b = -.192, $t(186)$ = -.880, p = .380. Without a significant effect of the independent variable on the mediator variable, the mediation effect is not possible. Therefore, the analysis was ended, resulting in no mediation. H14a was not supported.

H14b hypothesized a mediation effect of perceived usefulness onto the relationship between data evaluation and attitude. Therefore, a mediation test was conducted. In Step 1 of the mediation model, the regression of data evaluation on attitude towards Nozama, ignoring the mediator (perceived usefulness), was not significant, b = .153, $t(186)$ = .86, p = .392. Step 2 showed that the regression of data evaluation on the mediator, perceived usefulness, was marginally significant, b = .392, $t(186)$ = 1.80, p = .073. Step 3 of the mediation process showed that the mediator (perceived usefulness), controlling for data evaluation, was not significant, b= -.045, $t(186)$ = -.32, p = .752. Step 4 of the analyses revealed that, controlling for the mediator (perceived usefulness), data evaluation was a significant predictor of attitude towards Nozama, b = .504, $t(186)$ = 10.57, p <.001. These results show that data evaluation is not a predictor of perceived usefulness although Step 1 showed significant and Step 2 showed marginally significant effects. It was found that perceived usefulness did not mediate the relationship between data evaluation and attitude towards Nozama. H14b was not supported. The visualization of the mediation analysis can be found in Figure 4 below.

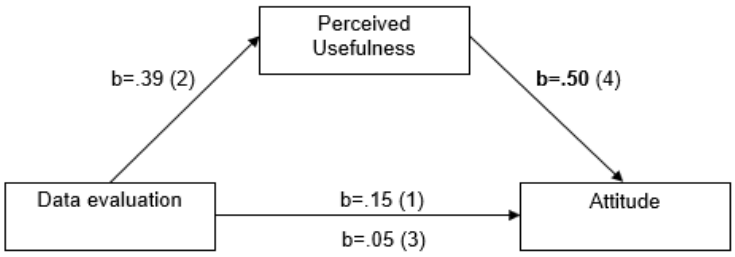


Figure 4
Mediation analysis of data evaluation on attitude by perceived usefulness

Privacy Concerns

It was also hypothesized that privacy concerns have a mediation effect on the relationship between voice activation and attitude towards Nozama. Step 1 of the mediation model shows that the regression of voice activation on attitude towards Nozama, ignoring the mediator (privacy concerns), was not significant, b = -.232, t(186) = -1.313, p = .191.Then, Step 2 showed that the regression of voice activation on the mediator, privacy concerns, was not significant, b = -.045, t(186) = -.367, p = .714. These results show that voice activation is not a predictor of privacy concerns. It was found that privacy concerns did not mediate the relationship between voice activation and attitude towards Nozama. Therefore, H15 was not supported.

Additionally, a mediation analysis for the effect of privacy concerns on the relationship of data evaluation and attitude was conducted. In Step 1 of the mediation model, the regression of data evaluation on attitude towards Nozama, ignoring the mediator (privacy concerns), was not significant, b = -.153, t(186) = .858, p = .392. Step 2 showed that the regression of data evaluation on the mediator, privacy concerns, was not significant, b = -.075, t(186) = .613, p = .541. This outcome resulted in the rejection of H15b. It was found that privacy concerns did not mediate the relationship between data evaluation and attitude towards Nozama.

Trust

It was assumed that trust mediates the relationship between voice activation and attitude towards Nozama. In Step 1 of the mediation model, the regression of voice activation on attitude towards Nozama, ignoring the mediator (trust), was not significant, b = -.232, t(186) = -1.313, p = .191. Step 2 showed that the regression of voice activation on the mediator, trust, was not significant, b = -.005, t(186) = .031, p = .976. Thus, H16a was not supported because it was found that trust did not mediate the relationship between voice activation and attitude towards Nozama.

Additionally, the mediation effect on voice activation was tested. In Step 1 of the mediation model, the regression of data evaluation on attitude towards Nozama, ignoring the mediator (trust), was not significant, b=-.153, t(186) = -.858, p = .392. Step 2 showed that the regression of data evaluation on the mediator, trust, was not significant, b=-.226, t(186) = -.1.362, p = .175. It was found that trust did not mediate the relationship between voice activation and attitude towards Nozama. Therefore, H16b was also rejected.

Table 11 shows an overview with the outcomes of the hypotheses testing.

Table 11
Overview of hypotheses testing

	Hypothesis	**Results**
H1	High perceived usefulness positively affects the attitude towards smart speakers.	Supported
H2	High privacy concerns negatively affect the attitude towards smart speakers.	Supported
H3	High trust in the service provider positively affects the attitude towards smart speakers.	Supported
H4	The attitude towards smart speakers is higher when voice activation is intentional (compared to unintentional).	Not supported
H5	The attitude towards smart speakers is higher when the data is evaluated by software (compared to humans).	Not supported
H6	Perceived usefulness is higher when the smart speaker is activated intentionally (compared to unintentionally) by voice.	Not supported
H7	Perceived usefulness is higher when the data on the smart speaker is evaluated by humans (compared to software).	Partially supported
H8	Privacy concerns are higher when the smart speaker is activated unintentionally (compared to intentionally) by voice.	Not supported
H9	Privacy concerns are higher when the data on the smart speaker is evaluated by humans (compared to software).	Not supported
H10	Trust in the service provider is higher when the smart speaker is activated intentionally (compared to unintentionally) by voice.	Not supported
H11	Trust in the service provider is higher when the data on the smart speaker is evaluated by software (compared to humans).	Not supported
H12	When data evaluation is done by humans (compared to software), privacy concerns are higher when the smart speaker is activated unintentionally than intentionally.	Not supported
H13	Trust in the service provider is higher when the data is evaluated by humans than by software when the smart speaker is activated intentionally (compared to unintentionally).	Partially supported
H14a	Perceived usefulness mediates the effect of voice activation on the attitude towards smart speakers.	Not supported
H14b	Perceived usefulness mediates the effect of data evaluation on the attitude towards smart speakers.	Not supported
H15a	Privacy concerns mediate the effect of voice activation on the attitude towards smart speakers.	Not supported
H15b	Privacy concerns mediate the effect of data evaluation on the attitude towards smart speakers.	Not supported
H16a	Trust in the service provider mediates the effect of voice activation on the attitude towards smart speakers.	Not supported
H16b	Trust in the service provider mediates the effect of data evaluation on the attitude towards smart speakers.	Not supported

5. Discussion

In this chapter, the results of the direct effects of perceived usefulness, privacy concerns and trust on attitude will be discussed. Furthermore, this study investigated the effect of voice activation (intentional vs. unintentional) and data evaluation (by software vs. by humans) on attitude towards Nozama (as a fictional example of a smart speaker brand). Moreover, it was expected that perceived usefulness, privacy concerns, and trust mediate the effects of the independent variables on the dependent variable.

The following section discusses the findings, implications, and limitations of the research as well as future recommendations for following studies in the field of smart speakers and voice technologies.

5.1. Discussion of the results

5.1.1. Effects of perceived usefulness, privacy concerns, and trust

Corresponding to the literature, direct effects of perceived usefulness, privacy concerns, and trust on attitude were found. In general, participants expressed their high privacy concerns, low trust and attitude and rather low perceived usefulness. While they knew what a smart speaker was, only half of participants had already used one. This could be an explanation for the high privacy concerns and distrust. Non-users seem to have a high skepticism towards smart speakers which could have arisen through media reports in which smart speakers were accused of having low data security (Day et al., 2019). Consequently, non-users already form a negative attitude without ever using such devices.

The results indicate that perceived usefulness influences attitude. This means that potential owners who value the convenience of smart speakers have a more positive attitude. Mostly, non-owners have low perceived usefulness which results in a less positive attitude towards Nozama. This outcome is in line with the study of Princi and Krämer (2019) who found out that convenience positively affects the willingness to deploy a smart device.

Besides, the negative effect of privacy concerns on attitude in the present study partially confirms former literature. For instance, the study of Chhetri and Motti (2019) investigated privacy concerns in detail and pointed out that always listing devices with tracking capabilities highly influences attitude. Controversy, Princi and Krämer (2019) did not find an effect of privacy concerns (towards tracking of devices) on willingness to adopt. This difference can be explained by the fact that their study was about smart vacuum cleaners and not smart speakers which seem to be more intrusive for users. Additionally, Menard and Bott (2018) claimed that privacy concerns towards smart home equipment results from the adoption. The present study proves that at least for smart speakers this is not true and non-users already have privacy concerns which influence attitude and lead to a more negative orientation.

Regarding trust, the present research indicates that higher trust leads to a more positive attitude and vice versa. This outcome is justified by other studies from Worthy et al. (2016) and Zheng et al. (2018) who came to the same conclusion and proved that trust is known for influencing attitude of IoT users.

The correlation analysis showed that perceived usefulness, privacy concerns, and trust are strongly correlated to attitude towards Nozama. Nevertheless, the data analysis does not allow any conclusions to be drawn about the time order and interrelatedness of these variables. Since the three independent variables (perceived usefulness, privacy concerns, and trust) could also be part of the overall attitude or overlap with attitude, one must be careful with specifying the hypothesized direction of the interrelatedness of the variables. The relationship between the variables could reasonably go the other way around. For example, although high privacy concerns and low trust lead to a lower attitude, it is possible that participants formed a low attitude towards smart speakers and therefore have high privacy concerns and low trust. The same argument can be applied on perceived usefulness since participants could perceive a higher usefulness of smart speakers' because they have a favorable attitude. Therefore, the conclusions of the regression analysis should be treated with caution. However, since the present study is based on former literature, there is theoretical evidence of the impact of perceived usefulness (Kowalczuk, 2018), privacy risks (Kowalczuk, 2018, Menard & Bott, 2018) and trust (Yang & al., 2017) on attitude towards smart home devices which confirm the results.

5.1.2. Effects of intrusive technology features

In the online experiment, participants were presented with a scenario design including intrusive technology features (voice activation and data evaluation) of an imaginary smart speaker (Nozama).

At first stance, the findings show that people do not seem to care whether the smart speaker gets activated unintentionally or intentionally and whether the data is evaluated by software or humans. Based on previous studies (Ayyagari et al., 2011; Benlian et al., 2019), it was expected that unintentional voice activation would lower the perceived usefulness of smart speakers as well as trust in the service provider and the attitude towards the devices and in turn would raise more privacy concerns. Unintentional voice activation can lead to a misfit between privacy concerns and perceived usefulness as stated by the authors (Benlian et al., 2019). Actual users of smart speaker claim that an unintentional activation of their device is perceived as strongly intrusive (Lau et al., 2018). On the contrary, the present study found that unintentional voice activation did not negatively influence attitude, perceived usefulness, and trust and had no positive effects on privacy concerns. The difference to former studies may be justified by the fact that the present study focused on potential consumers while Benlian et al.

(2019) investigated individuals who already owned a smart speaker. In contrast to users who are most likely already familiar with unintentional voice activations, non-users might not know about the device's functions and do not foresee the implications of activating it unintentionally (e.g. private conversation recording). Presumably, vignette scenarios were more realistic for users in the study of Benlian et al. (2019) since they could comprehend the situation better than non-users in the present study. This could also be the reason why there is no difference between groups of intentional and unintentional voice activation. Lau et al. (2018) interviewed owners and non-owners of smart speakers but only asked actual owners about the intrusiveness of unintentional voice activation. This might be an indicator for the difference to the present research as well as for the difference in methodology because the authors used a qualitative approach.

Additionally, it was expected that data evaluation by humans leads to an increase of privacy concerns and perceived usefulness and decreases trust in the service provider. Furthermore, a direct negative effect of data evaluation by humans on attitude was expected in line with literature from Malkin et al. (2019) who found that data evaluation by computers was more accepted. Opposed to this, no positive effects of data evaluation by humans on privacy concerns and no negative effects on attitude and trust were found. The difference to the former study can be explained by the same argument mentioned above: Malkin et al. (2019) surveyed actual smart speaker users who were probably more familiar with data evaluation practices. Furthermore, low trust and attitude and high privacy concerns already show that participants formed a negative stance towards smart speakers which indicates that they do not care about the type of data evaluation anymore.

However, perceived usefulness was marginally higher when the process of data evaluation in the experiment was claimed to be done by humans and not by machines. This result seems to indicate that non-owners value the usefulness of smart speaker higher if their voice data is evaluated by employees and not by software. An explanation for this is that non-users might expect the quality of Nozamas voice understanding to be better when the data is analyzed by humans rather than by machines. Non-owners seem to be aware of smart speaker companies' data processing practices. These companies often state that data evaluation by employees is needed for the devices' quality improvement. Non-users might support this practice in terms of usefulness because they might assume that human evaluation of voice data could improve the quality of smart speakers. They might also worry that autonomous big data analysis by software will result in errors which would lower smart speakers' usefulness. Malkin et al. (2019) elaborated on the effect of data evaluation by humans but did not related it to perceived usefulness. Therefore, this outcome gives new insights on how non-users of smart speakers perceive the usefulness of data evaluation by humans.

5.1.3. Interaction effects

It was assumed that two intrusive technology features (unintentional voice activation and data evaluation by humans) would result in higher privacy concerns than only one intrusive feature. Findings cannot prove this outcome probably because one intrusive feature alone did not have impact on privacy concerns.

Surprisingly, in the condition with intentional voice activation, trust in the smart speaker service provider was higher when data evaluation was done by humans compared to data evaluation by software. In the condition with unintentional voice activation, the results showed that participants' trust in the smart speaker service provider was approximately the same for both data evaluation by software and by humans. This outcome indicates that non-users of smart speakers perceive both types of data evaluation equally as bad when the smart speaker is activated unintentionally. They distrust the device regardless of whether data evaluation is done by software or by humans. An explanation for this is that unintentional voice activation leads to a breach of trust and that potential consumers do not care about the data evolution process anymore. Their trust in the service provider decreased in any way.

However, if the smart speaker is activated intentionally, the type of data evaluation does play a role. Participants still generally distrust the service provider of the smart speaker, but this distrust is even higher when their data is evaluated by a software. In other words, they have more trust in the smart speaker service provider when their data is evaluated by humans. This outcome contradicts former literature which often states that people perceive machines or software as more trustworthy than humans especially when it comes to cybersecurity (Hurtz, 2019; Ray, 2019; Winder, 2019). The result is also not in line with research of Malkin et al. (2019) who found that smart speaker users preferred their data to be reviewed by computers for quality control purposes and did not want employees to listen to their speech data.

Several reasons can be found for the discrepancy between the findings of this study and other research findings. First, the sample in this study consisted of non-owners. In the study of Malkin et al. (2019) actual smart speaker owners were surveyed. Possibly, non-owners distrust data evaluation by machines especially when the smart speaker is activated intentionally which means that everything works smoothly. Also, considering the other results, participants seem to have a negative stance towards smart speakers which can be transferred to a negative orientation towards technology in general. Therefore, they might trust machines processing their speech data even lesser than humans.

Besides, the survey of Malkin et al. (2019) was conducted before the media published reported about Amazon workers listening to users' voice recordings. This could mean that users were not aware of the fact that employees could possibly assess their voice recordings. Since the present study was conducted at a later point in time, it could mean that consumers are now more familiar with human data evaluation. The media reports about the data

processing technique of IoT device companies might have resulted in raising people's awareness which in turn resulted in more understanding and trust towards smart speaker companies regarding data evaluation by humans. As Hurtz (2019) states in his article, machines can improve their skills independently with deep learning methods, but completely autonomous systems are rare and voice assistants need human ears for support.

Second, some people are reluctant to trust machines or software when it comes to moral decisions (Crockett, 2017). Even if the intentional voice activation was not connected to a moral issue, people might expect to have an employee evaluate their voice recordings when they ask for information or give a request. This mental process can be illustrated by a car driver asking a navigation device for the correct route. People might have more trust when they know that this route was calculated because of data evaluation by humans compared to software. This cognitive process might be applicable to smart speakers as well.

However, with all these results, it is important to mention that trust in the smart speaker service provider was on average rather low. Even though it seemed like trust was higher for human data evaluation when the smart speaker was activated intentionally, participants still had low trust in general.

5.1.4. Mediation effects

Contrary to the expectations, there were no mediation effects of perceived usefulness, privacy concerns, and trust on the relationship between the independent variables and the dependent variable. Perceived usefulness, privacy concerns, and trust are usually known to be predictors for attitude towards smart speakers in general (Fruchter & Liccardi, 2018; Pridmore et al., 2019) which was confirmed by the regression analysis. In the present research it was expected that these variables would also act as mediators for the effect of voice activation and data evaluation on attitude. However, mediation effects could not be proven. This outcome might be due to the other results since both intrusive features did not directly influence attitude and most of the other variables.

5.2. Implications

Based on the findings of this study, both theoretical and practical implications can be made.

Theoretical implications

From the theoretical perspective, this study adds new findings to the field of IoT attitude and perceptions with regards to smart speakers. Thereby, this study was the first that investigated the effects of voice activation and data evaluation on specific variables based on the TAM and

the privacy calculus model. The present study integrated factors evolving around privacy from both models, thereby combining them. The results validated the capacity of the TAM in the smart speaker context although the applicability of the privacy calculus could not be proven. The findings of the main effects of perceived usefulness, privacy concerns, and trust can be attributed to the TAM. As in extended models of the TAM, privacy concerns or perceived privacy risks and trust proved to influence technology attitude (Dhagarra, Goswami, & Kumar, 2020; Yang & Lee 2018; Zhang et al., 2019) next to perceived usefulness as in the original model (Davis, 1989). Therefore, an integration in the technology acceptance model by Davis (1989) proved to be well grounded. In this way, the addition of privacy concerns and trust to the original model as well as the applicability to smart speakers of previous studies is confirmed by the present study.

Furthermore, the direct effects of perceived usefulness, privacy concerns, and trust provide theoretical implications in demonstrating which variables can influence attitude towards smart speakers. Nevertheless, there is no evidence for the proposed effect of the privacy calculus model in which privacy concerns can be outweighed by the benefits of a product (Majumdar & Bose, 2016). Applied to this study, intentional voice activation should have resulted in higher perceived usefulness (compared to unintentional voice activation) which would have outweighed high privacy concerns and lead to a positive attitude. Since there was no difference in outcomes of unintentional and intentional voice activation on privacy concerns, the privacy calculus model does not apply in this context.

Additionally, this research further contributed to the investigation of intrusive technology features which is a response to an appeal in research (Ayyagari et al., 2011). By finding marginal proof of the effects of data evaluation on perceived usefulness and of voice activation and data evaluation on trust, this study provides insights into intrusive technology features are perceived by potential owners of smart speakers.

Practical implications

One of the main practical contributions of the study are the findings on factors which influence the attitude for potential owners. This can help companies and developers in the IoT industry in several ways. First, with regards to perceived usefulness, higher attention should be drawn towards demonstrating the usefulness and benefits of smart speakers to (potential) consumers. This can be realized by developing effective marketing strategies. If implemented, non-users might be persuaded by the convenience of smart speakers and might develop a more positive attitude which can result in the adoption or intention to use a smart speaker.

Second, the disclosure of data evaluation and processing techniques remains important. If companies and service providers would publish information about the data processing and storage of smart speaker, this could lower the privacy concerns of non-users. It is

highly important to ensure the security of (voice-) data since it can lower the privacy concerns which would in return influence the attitude towards smart speakers.

Third, the present research proves that trust also effects attitude. This indicates that more trust in technology companies needs to be established. Through marketing strategies and good reputation management, technology companies and service providers can build up trust in their products and address more consumers. The more trustworthy potential consumers perceive the smart speaker, the more positive will they have a positive attitude towards the product which can lead to its adoption.

Finally, attention should be paid to the effects of the intrusive technology features. Human data evaluation is not perceived as intrusive as expected. This might result from the media coverage of these data analysis practices making consumers more familiar with data evaluation by employees. Experts should continuously observe privacy perceptions of consumer since they can change over time (Iachello & Hong, 2007). Smart speaker companies should consider being more honest about their data handling because it can have positive outcomes.

Taken together, the results of this study can help researchers, smart speaker developers and companies in designing smart speakers and guidelines for data security and processing techniques. A special emphasis should be put on the perceptions and attitudes of non-users who could become potential smart speaker owners.

5.3. Limitations and future research

The data analysis has also shown some limitations of this study which need to be considered in future research. Concerning the methodology, participants were provided with an imaginary scenario. Hypothetical situations are limited by design since they are only theoretically possible and do not reflect the reality in all its facets. Nevertheless, the vignettes were created as realistically as possible using detailed information. Additionally, imaginary scenarios are important for testing effects of potential situations with IoT devices. It seems like non-owners generally did not understand the different consequences of unintentional or intentional voice activation and of data evaluation by software or employees. In future research, more attention should be paid to the fact that non-user might have difficulties in understanding fictive scenarios with smart speakers. More experiments are needed wherein participants are provided with a more realistic context with actual smart speakers. Qualitative research like focus groups or interviews are also a solution to understand underlying connections of attitudes.

Furthermore, the vignettes only showed specific situations which can be different from the reality and depend on the specific brand of smart speaker. For example, the data handling varies by companies and countries. While, strict rules are valid for the data processing apply

in some countries, companies have more freedom in other countries. Thus, if the data is evaluated by both software and employees or only by one type is on the company's side.

The marginally significant effects of the intrusive features on perceived usefulness and trust seem to show that the technology acceptance model can be expanded and that intrusive features of technology are relevant for consumers' acceptance of technology. Further research about these features is necessary. Other intrusive features like cloud data storage which results in smart speakers' learning of users' daily routines or the possibility of data theft by hackers (Jackson & Orebaugh, 2018) should be considered as well.

Next to that, only the factor attitude towards Nozama was used for analysis, attitude towards smart speakers had to be deleted due to the loading of several factors in one construct. Consequently, the assumptions in this study refer to the attitude towards one specific smart speaker brand which is imaginary because it was invented by the researcher. Therefore, the conclusions which were drawn may deviate if the same study would have been carried out with another (famous) smart speaker brand (e.g. Amazon Echo).

Due to the concentration on smart speakers as one IoT device, general conclusions on other IoT devices should be treated with caution. Future research should investigate different IoT devices and elaborate on specific differences resulting from their various functions. Furthermore, unintentional voice activation also depends on the type of smart speaker, since some have proven to be better in language processing than others (Lobe, 2017). In future research focussing on one specific brand and its individual intrusive features and characteristics would be of high interest and relevance.

Besides, the present research found evidence that non-users have a rather negative attitude towards Nozama, which suggests that attitudes towards smart speakers are generally rather negative. Low perceived usefulness, low trust, and high privacy concerns influence this effect. Other factors like perceived ease-of-use, social influence or costs were not considered in this research but might also have an effect. Furthermore, only attitude was incorporated as a dependent variable. In the original TAM the actual product or system forms the endpoint in the model which is reached by behavioural intention which is again reached by attitude as a general impression. Thus, the results do not provide insight into all facets which could influence attitude towards smart speakers. Additionally, it only focussed on attitude and did not focus on the continuative variable's *behavioural intention* and *actual use*. In future research, this aspect needs to be considered through integrating more relevant factors of the TAM model and other models which might play a role.

5.4. Conclusion

This empirical study aimed to investigate whether unintentional voice activation (compared to intentional) and data evaluation by humans (compared to software) negatively influence the attitude towards smart speakers. Nozama, a fictional smart speaker, was used as an example of an IoT technology. Thereby, this study also examined the perceived usefulness, privacy concerns, and trust as independent and mediating variables.

The most important finding is the established fact that participants generally have a strong negative mindset towards Nozama which is represented by low perceived usefulness, low trust and attitude, and high privacy concerns. Contrary to the expectations, there was no difference in effects regarding the type of voice activation or data evaluation practice. Nevertheless, is seems like data evaluation by software leads to a lower perceived usefulness than data evaluation by humans. The study suggests that consumers are more skeptical towards machines when it comes to data processing. The same applies for trust. When the smart speaker is activated intentional, consumers seem to distrust machines even more than humans.

The findings can be used as an inspiration and basis for the growing field of IoT technology and are relevant for smart device developers and technology companies. Since smart speakers are perceived as relatively negative by non-users, new strategies are needed to reach this group. In addition, the study established that the investigation of non-users is highly relevant as there are different outcomes compared to former studies which only examined owners of smart speakers.

What will happen in the future remains to be seen. What is certain is that the relevance of voice technology will increase in the future and that the technology industry must dray more attention towards the consumers' needs.

References

Al-Heeti, A. (2019). *Echo effect: US smart speaker ownership nearly doubles in a year, survey says*. CNET. Retrieved 19 February 2020, from https://www.cnet.com/news/echo-effect-smart-speaker-ownership-nearly-doubles-in-a-year-survey-says/.

Aguinis, H., & Bradley, K. (2014). Best Practice Recommendations for Designing and Implementing Experimental Vignette Methodology Studies. *Organizational Research Methods*, *17*(4), 351-371. https://doi.org/10.1177/1094428114547952

Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: Technological Antecedents and Implications. *MIS Quarterly*, *35*(4), 831-858. https://doi.org/10.2307/41409963

Baumer, E., Burrell, J., Ames, M., Brubaker, J., & Dourish, P. (2015). On the importance and implications of studying technology non-use. *Interactions*, *22*(2), 52-56. https://doi.org/10.1145/2723667

Beldad, A., Jong, M. D., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior, 26*(5), 857-869. https://doi:10.1016/j.chb.2010.03.013

Beldad, A., & Hegner, S. (2017). Expanding the Technology Acceptance Model with the Inclusion of Trust, Social Influence, and Health Valuation to Determine the Predictors of German Users' Willingness to continue using a Fitness App: A Structural Equation Modeling Approach. *International Journal of Human–Computer Interaction*, *34*(9), 882-893. https://doi.org/10.1080/10447318.2017.1403220

Bennett, K., & Allen, P. (2012). *SPSS Statistics A Practical Guide Version 20*. (1st ed.) Cengage Learning Australia Pty Limited.

Benlian, A., Klumpe, J., & Hinz, O. (2019). Mitigating the intrusive effects of smart home assistants by using anthropomorphic design features: A multimethod investigation. *Information Systems Journal*. https://doi.org/10.1111/isj.12243

Blass, B. (2018). Wie Alexa & Co. den Alltag verändern. *Der Freie Zahnarzt*, *62*(11), 42-44. https://doi.org/10.1007/s12614-018-7534-0

Bleier, A., & Eisenbeiss, M. (2015). The Importance of Trust for Personalized Online Advertising. *Journal of Retailing*, *91*(3), 390-409. https://doi.org/10.1016/j.jretai.2015.04.001

Brush, A., Hazas, M., & Albrecht, J. (2018). Smart Homes: Undeniable Reality or Always Just around the Corner? *IEEE Pervasive Computing*, *17*(1), 82-86. https://doi.org/10.1109/mprv.2018.011591065

Chhetri, C., & Motti, V. G. (2019). Eliciting Privacy Concerns for Smart Home Devices from a User Centered Perspective. *Lecture Notes in Computer Science*, 91–101, *https://doi:10.1007/978-3-030-15742-5_8*

Choe, E., Consolvo, S., Jung, J., Harrison, B., & Kientz, J. (2011). Living in a glass house. *Proceedings of the 13Th International Conference on Ubiquitous Computing - Ubicomp '11*. https://doi.org/10.1145/2030112.2030118

Chung, H., Iorga, M., Voas, J., & Lee, S. (2017). "Alexa, Can I Trust You?". *Computer*, *50*(9), 100-104. https://doi.org/10.1109/mc.2017.3571053

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: Concepts, evolving themes, a model. *International Journal of Human-Computer Studies, 58*(6), 737-758. https://doi:10.1016/s1071-5819(03)00041-7

Crockett, M., Pizarro, D., & Everett, J. (2017, April 24). *Why are we reluctant to trust robots?* The Guardian. Retrieved 14 July 2020, from https://www.theguardian.com/science/head-quarters/2017/apr/24/why-are-we-reluctant-to-trust-robots.

Cyr, J. (2019). *Focus Groups for the Social Science Researcher*. Cambridge: Cambridge University Press. http://doi.org/10.1017/9781316987124

Davis, F., Bagozzi, R., & Warshaw, P. (1992). Extrinsic and Intrinsic Motivation to Use Computers in the Workplace1. *Journal of Applied Social Psychology*, *22*(14), 1111-1132. https://doi.org/10.1111/j.1559-1816.1992.tb00945.x

Davis, F., Bagozzi, R., & Warshaw, P. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, *35*(8), 982-1003. https://doi.org/10.1287/mnsc.35.8.982

Day, M., Turner, G., & Drozdiak, N. (2019, April 11*). Amazon Workers Are Listening to What You Tell Alexa*. Bloomberg. Retrieved February 19, 2020 from https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio

Dhagarra, D., Goswami, M., & Kumar, G. (2020). Impact of Trust and Privacy Concerns on Technology Acceptance in Healthcare: An Indian Perspective. *International Journal of Medical Informatics, 141*, 104164. https://doi:10.1016/j.ijmedinf.2020.104164

Dinev, T., Albano, V., Xu, H., D'Atri, A., & Hart, P. (2016). Individuals' Attitudes Towards Electronic Health Records: A Privacy Calculus Perspective. *Advances In Healthcare Informatics And Analytics*, 19-50. https://doi.org/10.1007/978-3-319-23294-2_2

Fruchter, N., & Liccardi, I. (2018). Consumer Attitudes Towards Privacy and Security in Home Assistants. *Extended Abstracts Of The 2018 CHI Conference On Human Factors In Computing Systems*. https://doi.org/10.1145/3170427.3188448

Ford, M., & Palmer, W. (2018). Alexa, are you listening to me? An analysis of Alexa voice service network traffic. *Personal And Ubiquitous Computing*, *23*(1), 67-79. https://doi.org/10.1007/s00779-018-1174-x

Fortes, N., Pagani, M., & Rita, P. (2017). The effects of privacy concerns, perceived risk and trust on online purchasing behaviour. *International Journal Of Internet Marketing And Advertising*, *11*(4), 307–329. https://doi.org/10.1504/ijima.2017.10007887

Edwards, J. R., Cable, D. M., Williamson, I. O., Lambert, L. S., & Shipp, A. J. (2006). The phenomenology of fit: Linking the person and environment to the subjective experience of person-environment fit. *Journal of Applied Psychology, 91*(4), 802–827. https://doi.org/10.1037/0021-9010.91.4.802

Gordon, K. (2019, October 17). *Topic: Smart speakers*. Statista. Retrieved 4 February 2020, from https://www.statista.com/topics/4748/smart-speakers/#dossierSummary__chapter1.

Gerber, N., Reinheimer, B., & Volkamer, M. (2018, August). Home sweet home? Investigating users' awareness of smart home privacy threats. In *Proceedings of An Interactive Workshop on the Human aspects of Smarthome Security and Privacy (WSSP)*.

Hoffman, D. L., & Novak, T. P. (2015). *Emergent experience and the connected consumer in the smart home assemblage and the Internet of Things*. Retrieved 4 February 2020 from http://ssrn.com/abstract= 2648786

Hurtz, S. (2020). *"Hey Google, wie viele Menschen hören mir zu?"*. Süddeutsche.de. Retrieved 4 February 2020, from https://www.sueddeutsche.de/digital/alexa-google-datenschutz-1.4535355-2.

Jackson, C., & Orebaugh, A. (2018). A study of security and privacy issues associated with the Amazon Echo. *International Journal of Internet of Things and Cyber-Assurance*, *1*(1), 91–99. https://doi.org/10.1504/ijitca.2018.090172

Jacobsson, A., & Davidsson, P. (2015). Towards a model of privacy and security for smart homes. *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*. https://doi:10.1109/wf-iot.2015.7389144

Joshi, A., Kale, S., Chandel, S., & Pal, D. (2015). Likert Scale: Explored and Explained. *British Journal of Applied Science & Technology*, *7*(4), 396-403. https://doi.org/10.9734/bjast/2015/14975

Kim, D., Park, K., Park, Y., & Ahn, J. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, *92*, 273-281. https://doi.org/10.1016/j.chb.2018.11.022

Kinsella, B. (2019, March 15). *Five Percent of Dutch Households Adopt Smart Speakers in Just 4.5 Months, Google Home is the Leader - Voicebot.ai*. Voicebot.ai. Retrieved 14 March 2020, from https://voicebot.ai/2019/03/15/5-percent-of-dutch-households-adopt-smart-speakers-in-just-4-5-months-google-home-is-the-leader/.

Kinsella, B. (2019, October 11). *Over 20% of UK Households Have Smart Speakers while Germany Passes 10% and Ireland Approaches That Milestone - Voicebot.ai*. Voicebot.ai. Retrieved 19 March 2020, from https://voicebot.ai/2019/10/11/over-20-of-uk-households-have-smart-speakers-while-germany-passes-10-and-ireland-approaches-that-milestone/.

Kowalczuk, P. (2018). Consumer acceptance of smart speakers: a mixed methods approach. *Journal of Research in Interactive Marketing*. doi:10.1108/jrim-01-2018-0022

Kummer, T., Recker, J., & Bick, M. (2017). Technology-induced anxiety: Manifestations, cultural influences, and its effect on the adoption of sensor-based technology in German and Australian hospitals. *Information & Management*, *54*(1), 73-89. https://doi.org/10.1016/j.im.2016.04.002

Iachello, G., & Hong, J. (2007). End-User Privacy in Human-Computer Interaction. *Foundations and Trends® In Human-Computer Interaction*, *1*(1), 1-137. https://doi.org/10.1561/1100000004

Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, stop recording": Mismatches between smart speaker privacy controls and user needs. In *Poster at the 14th Symposium on Usable Privacy and Security (SOUPS 2018)*.

Lobe, A. (2017, March 22*). Psst, der Lautsprecher hört mit!* Retrieved July 17, 2020, from https://tageswoche.ch/gesellschaft/psst-der-lautsprecher-hoert-mit/

Luhmann, N., Davis, H., Raffan, J., Rooney, K., & Luhmann, N. (1979). *Trust; and, Power* (1st ed.). Wiley.

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. https://doi.org/10.2478/popets-2019-0068

Majumdar, A., & Bose, I. (2016). Privacy Calculus Theory and Its Applicability for Emerging Technologies. *Lecture Notes In Business Information Processing*, 191-195. https://doi.org/10.1007/978-3-319-45408-5_20

Mayer, R., Davis, J., & Schoorman, F. (1995). An Integrative Model Of Organizational Trust. *Academy Of Management Review*, *20*(3), 709-734. https://doi.org/10.5465/amr.1995.9508080335

Menard, P., & Bott, G. (2018). Investigating Privacy Concerns of Internet of Things (IoT) Users. *AMCIS*.

Moloney, M., & Potì, V. (2013). A Behavioral Perspective on the Privacy Calculus Model. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2310535

Nguyen, D., Bedford, A., Bretana, A., & Hayes, G. (2011). Situating the concern for information privacy through an empirical study of responses to video recording. *Proceedings Of The 2011 Annual Conference On Human Factors In Computing Systems - CHI '11*. https://doi.org/10.1145/1978942.1979419

Olson, C., & Kemery, K. (2019). *2019 Voice report: Consumer adoption of voice technology and digital assistants (Rep.).*

Oulasvirta, A., Pihlajamaa, A., Perkiö, J., Ray, D., Vähäkangas, T., & Hasu, T. et al. (2012). Long-term effects of ubiquitous surveillance in the home. *Proceedings Of The 2012 ACM Conference On Ubiquitous Computing - Ubicomp '12*. https://doi.org/10.1145/2370216.2370224

Perez, S. (2018, March 7). *47.3 Million U.S. Adults have Access to a Smart Speaker, Report Says*. Social.techcrunch.com. Retrieved 7 January 2020, from http://social.techcrunch.com/2018/03/07/47-3-million-u-s-adults-have-access-to-a-smart-speaker-report-says.

Pridmore, J., Zimmer, M., Vitak, J., Mols, A., Trottier, D., Kumar, P., & Liao, Y. (2019). Intelligent Personal Assistants and the Intercultural Negotiations of Dataveillance in Platformed Households. *Surveillance & Society*, *17*(1/2), 125-131. https://doi.org/10.24908/ss.v17i1/2.12936

Princi, E., & Krämer, N. (2020). I Spy with my Little Sensor Eye - Effect of Data-Tracking and Convenience on the Intention to Use Smart Technology. *Proceedings Of The 53Rd Hawaii International Conference On System Sciences*. https://doi.org/10.24251/hicss.2020.171

Ray, A. (2019, May 14). The Machine Heuristic: Why People Trust Machines More Than Humans. Retrieved July 14, 2020, from https://www.pioneeringminds.com/machine-heuristic-people-trust-machines-humans/

Rabe, A. (2019). Mensch-Maschine-Kommunikation – Ein Paradigmenwechsel steht bevor. *Wirtschaftsinformatik & Management*, *11*(3), 160-161. https://doi.org/10.1365/s35764-019-00176-8

Rahim, A., Safin, S., Kheng, L., Abas, N., & Ali, S. (2016). Factors Influencing Purchasing Intention of Smartphone among University Students. *Procedia Economics And Finance*, *37*, 245-253. https://doi.org/10.1016/s2212-5671(16)30121-6

Sharma, S., & Crossler, R. (2014). Disclosing too much? Situational factors affecting information disclosure in social commerce environment. *Electronic Commerce Research And Applications*, *13*(5), 305-319. https://doi.org/10.1016/j.elerap.2014.06.007

Schumann, J., von Wangenheim, F., & Groene, N. (2014). Targeted Online Advertising: Using Reciprocity Appeals to Increase Acceptance among Users of Free Web Services. *Journal Of Marketing*, *78*(1), 59-75. https://doi.org/10.1509/jm.11.0316

Smirek, L., Zimmermann, G., & Beigl, M. (2016). Just a Smart Home or Your Smart Home – A Framework for Personalized User Interfaces Based on Eclipse Smart Home and Universal Remote Console. *Procedia Computer Science*, *98*, 107-116. https://doi.org/10.1016/j.procs.2016.09.018

Smith, H., Milberg, S., & Burke, S. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, *20*(2), 167. https://doi.org/10.2307/249477

Smith H.J., Dinev T., & Xu H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989. https://doi.org/10.2307/41409970

Weidman, J., Aurite, W., & Grossklags, J. (2019). On Sharing Intentions, and Personal and Interdependent Privacy Considerations for Genetic Data: A Vignette Study. *IEEE/ACM Transactions on Computational Biology and Bioinformatics, 16*(4), 1349-1361. https://doi:10.1109/tcbb.2018.2854785

Westin, Alan F. (1967), *Privacy and Freedom,* New York, NY: Atheneum.

Winder, D. (2019, July 19). *People increasingly trust machines more than humans to manage cyber-security*. Scmagazineuk.com. Retrieved 14 July 2020, from https://www.scmagazineuk.com/people-increasingly-trust-machines-humans-manage-cyber-security/article/1590049.

Wirth, J., Maier, C., & Laumer, S. (2018). The influence of resignation on the privacy calculus in the context of social networking sites: An empirical analysis. In European Conference on Information Systems (ECIS) (Eds.), *Proceedings of the 26th European Conference on Information Systems (ECIS)*. Portsmouth, UK, GB.

Wottrich, V., van Reijmersdal, E., & Smit, E. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, *106*, 44-52. https://doi.org/10.1016/j.dss.2017.12.003

Worthy, P., Matthews, B., & Viller, S. (2016). Trust Me. *Proceedings of the 2016 ACM Conference on Designing Interactive Systems - DIS '16*. https://doi:10.1145/2901790.2901890

Yang, H., & Lee, H. (2018). Understanding user behavior of virtual personal assistant devices. *Information Systems and E-Business Management*, *17*(1), 65-87. https://doi.org/10.1007/s10257-018-0375-1

Yang, H., Lee, H., & Zo, H. (2017). User acceptance of smart home services: an extension of the theory of planned behavior. *Industrial Management & Data Systems*, *117*(1), 68-89. https://doi.org/10.1108/imds-01-2016-0017

Yang, H., Yu, J., Zo, H., & Choi, M. (2016). User acceptance of wearable devices: An extended perspective of perceived value. *Telematics and Informatics*, *33*(2), 256-269. https://doi.org/10.1016/j.tele.2015.08.007

Yoon, C., & Kim, S. (2007). Convenience and TAM in a ubiquitous computing environment: The case of wireless LAN. *Electronic Commerce Research and Applications*, *6*(1), 102-112. https://doi.org/10.1016/j.elerap.2006.06.009

Zhang, T., Tao, D., Qu, X., Zhang, X., Lin, R., & Zhang, W. (2019). The roles of initial trust and perceived risk in public's acceptance of automated vehicles. *Transportation Research Part C: Emerging Technologies, 98*, 207-220. https://doi:10.1016/j.trc.2018.11.018

Zeng, E., Mare, S., & Roesner, F. (2017). End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)* (pp. 65-80).

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1-20. https://doi.org/10.1145/3274469

Zorn, N. (2020, January 18). Amazon Alexa nutzen und die Privatsphäre schützen. *House-controllers.* Retrieved on March 1. 2020 from https://www.housecontrollers.de/smart-home/amazon-alexa-nutzen-und-die-privatsphaere-schuetzen-tipps/

Appendix A

Material for the Vignette Scenarios in the Pre-Study

Im folgenden Szenario versetze dich bitte in die Lage von Tom, der seine Freundin Mary für einen Kochabend besucht. Mary hat kürzlich einen neuen intelligenten Lautsprecher von der Marke Nozama bekommen, den sie dir vorstellt. Sie ist sehr aufgeregt und betont, dass der Lautsprecher sogar die Lichter steuern kann. Der Lautsprecher kann mit dem Wort „Nozama“ aktiviert werden. Während ihr in der Küche kocht, stellen Mary und du mit dem intelligenten Lautsprecher den Timer für die Kochzeit ein und schalten die Musik per Sprachbefehl um. Alles, ohne die Hände zu benutzen.

Voice activation Version 1

Als ihr zu Ende gegessen habt und im Wohnzimmer sitzt, wird es bereits dunkel in der Wohnung. Du musst langsam nach Hause gehen und sagst: „Ok Mary, ich muss jetzt heim“/“Nozama, schalte das Licht ein“. Als Antwort auf deinen Satz, wird der intelligente Lautsprecher Nozama aktiviert und sagt: „Ok, ich schalte das Licht ein“ und das Licht geht an. Du nimmst deine Tasche und verabschiedest dich von Mary.

Unintentional	Intentional
	

Voice activation Version 2

Während ihr zu Abend esst, sprecht ihr über eine Freundin, die sich nach nur einer Woche Ehe wieder scheiden ließ. Mary erzählt dir die ganze Geschichte. Du sagst: „Was ein Drama!“/ „Nozama, wie viele Menschen lassen sich nach einer Woche Ehe wieder scheiden?“. Als Antwort auf deinen Satz wird der intelligente Sprecher Nozama aktiviert und sagt: "Ich konnte nicht herausfinden, wie viele Personen sich nach einer Woche Ehe wieder scheiden ließen." Mary sagt: „Wahrscheinlich mehr als wir denken“ und ihr wechselt zu einem anderen Gesprächsthema.

Unintentional	Intentional
	

Voice activation Version 3

Während des Abendessens erzählt Mary dir von ihrem harten Arbeitstag und beschreibt wie unfair ihr Chef sie behandelt. Du willst sie aufmuntern und sagst: „Komm, das wird schon wieder!“/“Nozama, spiel ein paar fröhliche Lieder“. Als Antwort auf deinen Satz wird der intelligente Lautsprecher Nozama aktiviert und sagt: "Ok, hier ist ein fröhliches Lied für Dich." Mary lacht und ihr beide hört euch noch ein paar Songs gemeinsam an.

Unintentional	Intentional
	

Data evaluation Version 1

Zurück zu Hause recherchierst du im Internet nach weiteren Informationen über den intelligenten Lautsprecher Nozama. Du stößt auf eine Erklärung eines Datenschutzbeauftragten.

Software	Humans
 "Always-on Geräte sammeln sehr intime Daten darüber, wohin wir gehen, mit wem wir Zeit verbringen, worüber wir sprechen und nachdenken. Sie sind Teil einer Überwachungskultur, genährt von Geschäftsmodellen, die unsere Daten verkaufen, und von Regierungen, die uns überwachen wollen », kritisiert ein IT-Sicherheitsexperte. Unternehmen können über den Lautsprecher viel über die Vorlieben ihrer Benutzer lernen. Um die Dienste der Geräte zu verbesser, landet jedes Wort auf einer Serverfarm, wo es von Software ausgewertet wird."	 "Always-on Geräte sammeln sehr intime Daten darüber, wohin wir gehen, mit wem wir Zeit verbringen, worüber wir sprechen und nachdenken. Sie sind Teil einer Überwachungskultur, genährt von Geschäftsmodellen, die unsere Daten verkaufen, und von Regierungen, die uns überwachen wollen », kritisiert ein IT-Sicherheitsexperte. Unternehmen können über den Lautsprecher viel über die Vorlieben ihrer Benutzer lernen. Um die Dienste der Geräte zu verbessern, werden die Daten von Mitarbeitern analysiert, die sich dazu die privaten Sprachaufnahmen anhören."

Data evaluation Version 2

Zurück zu Hause schaltest du den Fernseher ein und eine Dokumentation über intelligente Lautsprecher wird grade gezeigt. Der Dokumentarfilm erklärt den Speicherungs- und Analyseprozess der Sprachdaten auf intelligenten Lautsprechern und nennt Nozama als Markenbeispiel für intelligente Lautsprecher. Unter anderem wird der folgende Auszug gezeigt:

Software	Humans
 Jedes Wort landet auf einer Serverfarm, wo es von einer Software ausgewertet wird, um die Dienste von Nozama zu verbessern.	 Um die Dienste von Nozama zu verbessern, werden die Daten von Mitarbeitern analysiert, die sich dazu die privaten Sprachaufnahmen anhören.

Appendix B

Main Study

Dear respondent,

Thank you for taking the time to complete this survey. This experimental survey was invented for a study about smart speakers for my master's research at the University of Twente. It will take approximately 8 minutes to complete.

The experimental survey will contain a scenario with text and graphics. It is important that you fully read the instructions and answer the follow-up questions carefully.

It is an anonymous survey; all the information you provide is confidential and will only be used for this research. You may quit the experiment at any given time without explanation.

If you have any questions, please feel free to contact me (h.l.palenio@student.utwente.nl).

Thank you for your participation!
Hedda Palenio

Do you agree to participate in this survey?

- ○ Yes

What is your gender?

- ○ Male
- ○ Female
- ○ Other
- ○ Prefer not to say

How old are you?

Please indicate your nationality:

- ○ German
- ○ Dutch
- ○ Other:

Please read the information about smart speakers carefully if you don't know what a smart speaker is.

What is a smart speaker?

A smart speaker is a type of wireless speaker and voice command device with an integrated virtual assistant.

A smart speaker offers:

- hands-free activation with the help of one or more "wake-words"
- a variety of functions (controlling smart lights and other smart home services, ordering products, streaming/playing of music, etc.)
- works with artificial intelligence

Example of a smart speaker: Amazon Echo
Integrated virtual assistant: Alexa

Please answer the questions. With smart speakers we mean real speakers (not Siri or other virtual assistants on mobile phones).

Do you know what a smart speaker is?

- ○ Definitely yes
- ○ Probably yes
- ○ Might or might not
- ○ Probably not
- ○ Definitely not

Have you ever used a smart speaker?

- ○ Definitely yes
- ○ Probably yes
- ○ Might or might not
- ○ Probably not
- ○ Definitely not

Do you already own a smart speaker? (e.g. Amazon Echo, Google Home, Apple HomePod)

- ○ No
- ○ Yes

Do you plan to adopt a smart speaker in the future?

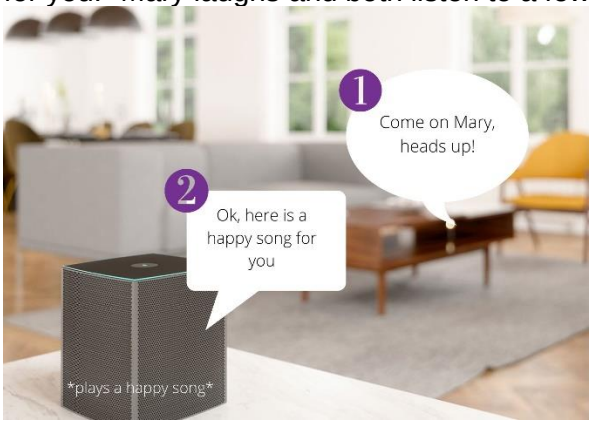
- ○ Definitely yes
- ○ Probably yes
- ○ May or may not
- ○ Probably not
- ○ Definitely not

Please imagine the following (imaginary) scenario and put yourself in the shoes of Tom.

Tom is visiting his friend Mary for an evening of cooking. Mary recently got a new smart speaker called Nozama which she presents to you. She is very excited and highlights that the speaker can even control the lights. The speaker can be activated with the wake words “Nozama”. While working in the kitchen, Mary and Tom use the smart speaker for setting the timer for the cooking time and switching music on their favourite playlist. All with free hands.

Condition 1: Unintentional voice activation*data evaluation by software
Condition 2: Unintentional voice activation*data evaluation by humans
Condition 3: Intentional voice activation*data evaluation by software
Condition 4: Intentional voice activation*data evaluation by humans

Intentional voice activation
During dinner, Mary tells Tom about her hard day at work and describes how unfairly her boss treated her. Tom wants to cheer her up and says: "Come on Mary, heads up!". In response to Tom's wordings, the smart speaker Nozama is activated and says: "Ok, here is a happy song for you." Mary laughs and both listen to a few songs together.



Intentional voice activation

During dinner, Mary tells Tom about her hard day at work and describes how unfairly her boss treated her. Tom wants to cheer her up and says: "Come on Mary, heads up!" In response to Tom's wordings, the smart speaker Nozama is activated and says: "Ok, here is a happy song for you." Mary laughs and both listen to a few songs together.

Data evaluation by software

Back home, Tom scrolls the Internet for more information about Nozama. He comes across a statement from a data protection expert:

"Always-on devices collect very intimate data about where you are going, who we are spending time with, what we are talking about and thinking about. They are part of a surveillance culture, fueled by business models that sell our data and governments that want to monitor us" criticizes an IT security expert. Companies can learn a lot about its users' preferences through its listening speaker. Every word which is directed to the speaker ends up on a **server farm**, where it is **evaluated by software (through computers)** for the purpose of improving the service of the device.

Data evaluation by humans

Back home, Tom scrolls the Internet for more information about Nozama. He comes across a statement from a data protection expert:

"Always-on devices collect very intimate data about where you are going, who we are spending time with, what we are talking about and thinking about. They are part of a surveillance culture, fueled by business models that sell our data and governments that want to monitor us" criticizes an IT security expert. Companies can learn a lot about its users' preferences through its listening speaker. For the purpose of improving the service of the device, the **data is evaluated by employees** who listen to your private recordings.

Remember the scenario that you read before and answer the questions about Nozama.

	Strongly agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
I have positive feelings about Nozama	○	○	○	○	○	○	○
Nozama is a great invention	○	○	○	○	○	○	○
I really like Nozama	○	○	○	○	○	○	○
My attitude towards Nozama is positive	○	○	○	○	○	○	○
I am really interested in Nozama	○	○	○	○	○	○	○

Please answer to what extent you agree or disagree with the statements below.

	Strongly agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
Using a smart speaker would give me convenience at home	○	○	○	○	○	○	○
Using a smart speaker would give me pleasure	○	○	○	○	○	○	○
I find smart speakers convenient in day-to-day life	○	○	○	○	○	○	○
Using a smart speaker would make my everyday life easier	○	○	○	○	○	○	○
It is great that smart speakers are customized to my personal needs	○	○	○	○	○	○	○

Please answer to what extent you agree or disagree with the statements below.

	Strongly agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
It is risky to disclose private information to a smart speaker	○	○	○	○	○	○	○
I am worried that smart speakers will store my private data	○	○	○	○	○	○	○
My private information on a smart speaker could be misused	○	○	○	○	○	○	○
Companies would collect too much personal information about me if I would use a smart speaker	○	○	○	○	○	○	○
I am concerned that smart speakers would track my private information	○	○	○	○	○	○	○

Please answer to what extent you agree or disagree with the statements below. With smart speaker service providers we mean the companies which offer the smart speaker and their service.

	Strongly agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
I think smart speaker service providers are reliable	○	○	○	○	○	○	○
I perceive smart speaker service providers as trustworthy	○	○	○	○	○	○	○
I think smart speaker providers keep customers' best interests in mind	○	○	○	○	○	○	○
I believe smart speaker service providers to be honest	○	○	○	○	○	○	○
I think smart speaker service providers keep promises and commitments	○	○	○	○	○	○	○

Please answer to what extent you agree or disagree with the statements below.

	Strongly agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
I have positive feelings about smart speakers	○	○	○	○	○	○	○
Smart speakers are a great invention	○	○	○	○	○	○	○
I really like smart speakers	○	○	○	○	○	○	○
My attitude towards smart speakers is positive	○	○	○	○	○	○	○
I am really interested in smart speakers	○	○	○	○	○	○	○

Now please think back to the scenario.

Tom has activated the smart speaker with the activation word (command): "Nozama"

- ○ True
- ○ False

Back home, Tom read an article about data collection of smart speakers. The analysis of the data is carried out (according to the article) by:

- ○ Humans
- ○ Software

Appendix C

Survey items

Constructs	Items	References
Perceived usefulness	Using a smart speaker would give me convenience at home	Princi and Krämer (2020); Yang and Lee (2019)
	Using a smart speaker would give me pleasure	
	I find smart speakers convenient in day-to-day life	
	Using a smart speaker would make my everyday life easier	
	It is great that smart speakers are customized to my personal needs	
Privacy Concerns	It is risky to disclose private information to a smart speaker	Kowalsczuk (2018); Yang, Lee and Zo (2017)
	I am worried that smart speaker will store my private data	
	My private information on a smart speaker could be misused	
	Companies would collect too much personal information about me if I would use a smart speaker	
	I am concerned that smart speakers would track my private information	
Trust	I think smart speaker service providers are reliable	Yang, Lee and Zo (2017)
	I perceive smart speaker providers as trustworthy	
	I think smart speaker providers like keep customers' best interests in mind	
	I believe smart speaker service providers to be honest	
	I think smart speaker service providers keep promises and commitments	
Attitude towards Nozama	I have positive feelings about Nozama	Fortes, Rita and Pagani (2017); Self-generated
	Nozama is a great invention	
	I really like Nozama	
	My attitude towards Nozama is positive	
	I am really interested in Nozama	

Attitude towards smart speaker	I have positive feelings about smart speakers Smart speakers are a great invention I really like smart speakers My attitude towards smart speakers is positive I am really interested in smart speakers	Fortes, Rita and Pagani (2017); Self-generated