The Perceived Surveillance of Conversations Through Smart Devices

Citation for published version:
Frick, NRJ, Wilms, KL, Brachten, F, Hetjens, T, Stieglitz, S & Ross, B 2021, 'The Perceived Surveillance of Conversations Through Smart Devices', *Electronic Commerce Research and Applications*, vol. 47, pp. 101046. https://doi.org/10.1016/j.elerap.2021.101046

Digital Object Identifier (DOI):
10.1016/j.elerap.2021.101046

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Publisher's PDF, also known as Version of record

Published In:
Electronic Commerce Research and Applications

THE PERCEIVED SURVEILLANCE OF CONVERSATIONS THROUGH SMART DEVICES

ABSTRACT

Organizations are collecting large amounts of data that are generated by internet-connected devices in people's homes. This raises questions regarding online privacy and data security. A common concern is that online advertisements are personalized based on conversations that have unknowingly been recorded by people's smart devices. The present article examines this phenomenon and the potential determinants influencing this concern. For this purpose, an online survey (N = 277) was conducted. Three predictors were identified that affect the perceived surveillance of conversations: trust in smart devices, computer anxiety and prior negative experience. The developed surveillance effect model is discussed to understand the factors influencing this concern. The findings of this study serve as a foundation for future research and might support organizations in optimizing customer relations.

Keywords: Surveillance effect, Perceived Surveillance of Conversations, personalized ads, online privacy concern, smart devices

1. Introduction

Digital data is widely described as the new currency of the digital economy. Online advertisers strive to expand data collection and monetize its targeted use in advertising (Mathews-Hunt, 2016; Ross et al., 2018). With different devices and applications, people leave commercially valuable digital tracks in exchange for online user experience, functionality and access (Hill, 2017). Various devices such as wearables, smartphones and other Internet-connected devices are able to collect private user information such as communication patterns (Andrejevic and Burdon, 2015), fitness parameters or physical location (Di Martino et al., 2018). By analyzing information such as shopping patterns, dining preferences and clubbing habits, complete profiles of consumers' lifestyles can be built, which can then be used for commercial purposes (Andrejevic and Burdon, 2015; Gironda and Korgaonkar, 2018). The individual actions of each consumer can be evaluated to serve targeted advertisements resulting in a better click rate (Aguirre et al., 2015).

Although personal data is obviously used for advertising purposes, it is often unclear to the affected individuals when personal data is tracked, where it is stored, with whom it is shared and how it is used. Understandably, questions concerning personal privacy and security arise (Bergström, 2015; Preibusch, 2013). The use of personalized ads especially leads to privacy concerns (Bleier and Eisenbeiss, 2015). While society is becoming more aware of data protection, general concerns about technical innovations have emerged which cannot always be substantiated. A common concern arises when consumers see personalized online ads for items or services that they have recently spoken about in offline conversations. The suspicion is that the conversation has been secretly recorded by a device such as a smartphone or a smart speaker and that the topic of this conversation is used to personalize the ad. Since smartphones and smart speakers are equipped with microphones and connected to the internet, these devices are technically able to record audio and transmit it to a server. These concerns seem to grow with the increasing spread of smart devices, which are activated by key phrases such as "OK Google" and "Hey Siri" and which therefore need to continuously analyze audio signals. People around the world report anecdotal evidence: Two people chatted about a tax issue and the following day, one of them was shown a Facebook ad for tax experts offering advice on the exact same issue

(Kleinman, 2016). In this case, some people would argue that Facebook has recorded audio over the smartphone's microphones and then used voice recognition software in order to be able to show relevant ads in the person's news feed (Guynn, 2018). However, there is no empirical evidence that conversations are secretly recorded. Companies such as Google (CBS, 2018) and Facebook (Facebook Inc., 2016) deny using audio data for advertising purposes and computer scientists have tested this assumption without finding supporting evidence in favor (Hill, 2017).

Research focusing on privacy concerns in the context of smart devices is still less explored but moving into the center of attention. Only few approaches for quantitative studies exist. McLean and Osei-Frimpong (2019) examined variables impacting the use of voice assistants (i.e., Amazon's Echo or Apple's Siri). Besides illustrating that individuals are motivated by utilitarian, symbolic and social benefits of systems, they also found that perceived privacy influences the use of assistants negatively. Lee et al. (2019) investigated that the post-adoption usage of Smart Voice Assistant Speakers positively impacts group harmony among users in a multi-person context. In addition, they also indicated that perceived security remains a concern but becomes less relevant when a device is already adopted. Besides the limited number of quantitative studies, scholars have mainly conducted qualitative research (Hoy, 2018; Lau et al., 2018; Siddike and Kohda, 2018). Studies examined the personal characteristics, sociodemographic factors and cognitive determinants that affect privacy concerns in an online environment in general (Bergström, 2015; Škrinjarić et al., 2018). Emami-Naeini et al. (2019) used interviews to show that privacy and security are major factors contributing to the decision of humans whether to purchase a smart device or not. Hoy (2018) outlined that privacy and security risks might reduce people's likelihood of adopting smart devices. Prior research also dealt with ads when using smart devices. Kim et al. (2018) identified that two-way communication with smart speakers is more effective than traditional one-way ads without any feedback. However, studies also indicate that people are afraid of smart devices listening in on conversations and that devices were even turned off before sleeping or before having private conversations (Abdi et al., 2019).

The above examples show that previous research was primarily concerned with factors focusing on the interaction with smart devices, especially related to usage behavior and adoption. However, it is still ambiguous what determines the concerns of users that their devices listen in on them and target them with ads based on recent conversations. This article broadens the understanding of data collection practices and people's privacy concerns, particularly the **perceived surveillance of conversations (PSoC)** by their smart devices. We develop theory to analyze the determinants of these concerns, which yields information on people's perceptions of how sensitive data is exploited and misused. The results can be used to learn more about how to inform users properly about privacy issues and how to educate them to ensure that they use smart devices, social media and online services responsibly. Providing a rational explanation might reduce the individual's feeling of being eavesdropped on. This might further clarify that smart devices are not listening in on conversations and companies are not using this information to provide targeted ads. The notion of PSoC, to our knowledge, has not seen sufficient research. Hence, the research question of this work is as follows:

RQ: Which individual factors influence the perceived surveillance of conversations?

To answer the research question, a structural equation model is developed that includes various variables that might affect the PSoC. The model is developed by combining factors from existing constructs in the related literature and new self-developed items. The relationships between constructs in the model are tested in an online survey.

This paper contributes to research and practice as one of the first forays explaining the phenomenon of the PSoC. We thereby provide a theory-based framework examining predictors in the context of smart devices. Researchers will find the insights fruitful in understanding the determinants of the PSoC, in particular, how trust in smart devices, risk beliefs, computer anxiety and prior negative experience contribute to this effect. Practitioners will be able to comprehend how suitable business-to-consumer relationships are established, ensuring the highest possible level of trust in vendors' devices. In terms of implications for society, readers will realize that the surveillance effect is influenced by several factors explaining the perception of smart devices secretly listening in on conversations. Hence, this article extends the information systems literature by updating our understanding about the impact of smart devices on individuals and the related effect of the PSoC.

2. Perceived Surveillance of Conversations

This research explores the PSoC, the perception of individuals that smart devices listen in on conversations to provide targeted ads that are displayed in social media feeds or websites.

2.1 Smart Devices

Smart devices are physical devices such as smartphones and smart speakers that are equipped with microphones and virtual assistants. In 2019, 134.8 million devices were sold worldwide, with projections of up to 200 million by 2023 (Statista, 2019). Amazon's Echo is the most popular one (Statista, 2020). Released in 2015, the Amazon Echo is a voice-controlled smart device that connects to Alexa, a virtual assistant service running on the vendor's server (Wu, 2018). Like Apple's Siri, Google Home and Microsoft Cortana, Alexa can be described as an intelligent voice-activated, cloud-based and screen-less service (Orr and Sanchez, 2018). These services can carry out various tasks such as retrieving information, checking scheduled calendar events, playing music, ordering food, controlling smart home devices, and more, after a verbal or typed command (Orr and Sanchez, 2018).

To be able to respond to voice commands, the technology requires sufficient processing capacities to handle the amounts of linguistic data (Wu, 2018). Recent advances in the machine learning algorithms used for comprehension of human-language input were a prerequisite for this development (Brachten et al., 2020; Mirbabaie et al., 2021; Wu, 2018). For the services to work properly, the smart devices are equipped with multi-directional microphones that constantly listen to their environment. However, according to the manufacturers, not all data collected is transferred to the server. For example, Amazon Echo buffers and re-records roughly every 1-3 seconds locally and only transmits data when it detects a specific sound pattern (Gray, 2017). Alexa then records the following request or question, which is processed by the virtual assistant service to provide a suitable response. This recording is stored on an Amazon server, which may be located outside the user's country (Orr and Sanchez, 2018). The data stored includes skills (app-like programs that can be installed on the assistant and enhance its capabilities to offer further services) which have been activated by the user, requests made to the Echo device including its response, general user information along with payment and shipping information and further details captured by third-party providers (Orr and Sanchez, 2018). Users have little influence on which personal data is processed at what time, through which services and in which locations. It has been reported that recordings are not only analyzed automatically, but also by humans, in order to improve the system. Consequently, concerns over trust and privacy have emerged, especially the question whether smart devices are "always on" and actively listening in on conversations.

2.2 The Surveillance Effect

A common and persistent concern is that smart devices are constantly listening to conversations and that ads on social media platforms, apps and websites are tailored to the topics talked about in the presence of such a device. Anecdotal evidence is reported by users from all over the world that immediately after talking about a certain product, advertising for this item was shown in their social media feed without ever searching for or writing about it (BBC, 2017; Kohut, 2018). Even if people are convinced that this data is exploited for the purpose of showing relevant ads (High, 2017), this perception might be a result of pure coincidence (BBC, 2017). The phenomenon that people worry that their smart devices listen in on them and relevant ads are displayed in social media feeds or websites based on recent conversation topics has not been named yet. We use the term **surveillance effect** to refer to this concern.

There is no empirical evidence so far that smart devices secretly listen to conversations and transmit these recordings to companies for the purpose of personalizing online ads. Facebook, for example, denies using the smartphone's microphone to gain information about users. An official press release states that ads are merely based on the user profile and individual activities (Facebook Inc., 2016). Google also claims that they do not use ambient sound from any device to target ads (CBS, 2018). Furthermore, scientists analyzed the data traffic that was sent by popular smartphone apps including Facebook. Even though they did find several apps leaking camera images and screen content over the Internet without the user's knowledge as well as apps that requested access to microphone and camera, no secretly recorded audio data was found (Pan et al., 2018). In an analysis of technical aspects such as network usage, sent data packages, CPU usage, microphone awake state logging and even power consumption, such a misuse of data could not be detected (KC Online Media, 2017). While the technical prerequisites might exist, this study's focus does not lie on confirming or debunking this suspicion but on its perception and how it affects the users' actions.

Psychological concepts that might be related to the surveillance effect, which initially seem to serve as possible explanations, are selective attention and confirmation bias. First, salient items are more likely to be noticed and others disregarded (Klayman, 1995). Second, people look for evidence that supports their existing beliefs and ignore potential counterevidence (Nickerson, 1998). Selective attention in particular means that our limited cognitive processing capacity is directed towards only some of the sensory input we receive (Stevens and Bavelier, 2012). Some stimuli are more salient than others, which thus may be disregarded. People's attention is then dominated by one thing rather than another (Driver, 2001). This effect is not a characteristic of the stimulus itself but of the person who perceives the stimulus. Items that individuals have already been exposed to, determine what they are going to perceive. In plain terms, the human eye sees what the brain is prepared to see.

Transferred to the surveillance effect, a logical explanation for its occurrence may be coincidence: A previously overlooked ad is only noticed after a conversation on the topic and thus becomes salient (Hassan, 2018). Every time a website, app or social media site is used, the user is confronted with various ads. Some of them have not been noticed previously as they seem irrelevant for the individual and therefore not salient. In contrast, an ad for a product that the user talked about recently stands out relative to the others. The attention is drawn to this ad, making the user wonder whether a previous conversation was somehow recorded by a smart device. Once suspicious, the user becomes even more attentive towards these incidentally relevant ads.

While the constructs of selective attention and the confirmation bias may serve as general explanations for a predisposition to pay attention to a stimulus, these constructs are insufficient in determining what factors exactly influence the forming of the perception that a conversation might be recorded by smart devices. Confirmation bias explains why people ignore evidence that contradicts their existing beliefs (Klayman, 1995; Nickerson, 1998), but it does not explain why they have these beliefs in the first place (for example, the belief that private conversations are being exploited for advertising purposes). Selective attention explains why people are more likely to notice an ad for something they have recently talked about (Driver, 2001; Florack et al., 2020), and it might therefore explain where they get the initial idea that their conversation was monitored, but it does not explain why some consider it plausible while others discard it as a fiction. To really ascertain why individuals believe that conversations are recorded for the purpose of tailoring ads, we cannot be satisfied with this simplistic explanation. Selective attention or confirmation bias offer a macro view and explain the occurrence of the effect in general. However, we argue that there is an urgent need for a more detailed micro view identifying individual factors explaining the predispositions in the user itself. Concrete research that examines what causes individuals to be convinced of being continuously monitored by smart devices is sparse and, in this regard, it is unclear why people believe that data is being misused for advertising purposes.

3. Related Work

While selective attention and confirmation bias may explain the occurrence of the surveillance effect in users, to understand if and why some people are more affected by this phenomenon than others and what influences these differences, a different approach needs to be considered.

3.1 Online Privacy Concerns

With the World Wide Web as a new technology in the 1990s, businesses began to share and exchange personal information. This led to increased concerns about privacy (Junglas et al., 2008). Smith et al. (1996) first constructed a measure that identifies the dimensions of individuals' concerns about organizational information privacy practices which has been validated by Stewart and Segars (2002). It includes the measures of collection of personal information, unauthorized access to personal information, deliberate and accidental errors in personal data and secondary use, which described a situation in which gathered data is not used for its intended purpose. At the beginning, online privacy concerns were mainly investigated in an organizational setting (Smith et al., 1996; Stewart and Segars, 2002). More recent research has focused on various contexts such as social media, online banking, websites, e-commerce, e-mailing, and mobile advertising (Bandyopadhyay, 2011; Bergström, 2015; Okazaki et al., 2009; Xu et al., 2008).

In many studies, the consequences of online privacy concerns have been examined. Bandyopadhyay (2011) found that the motivation to supply personal information to online shops and engage in the purchase of products was decreased by privacy concerns. Furthermore, Bansal et al. (2010) confirmed that disclosing health information to web-based healthcare services depends on the individuals' privacy concerns. Users' perceived security has been found to positively influence the willingness to share information on Facebook (Dhami et al., 2013). Also, the impact of privacy concerns on the adoption of new technology has been analyzed. Hsu and Lin (2016) demonstrated that privacy concerns can influence the intention to use services provided by the Internet of Things. A study on the adoption of location-based services indicates that privacy concerns influence perceived risk and trust, which in turn predict the intention to use location-based services (Zhou, 2011). A recent study by Anic et al. (2019) furthermore provides evidence that online privacy concerns negatively affect the willingness to share personal information.

As smart devices and intelligent personal assistants have only become widespread in the past five years, research on privacy concerns in this specific area is still sparse in contrast to research on general online privacy concerns. While general online activity is consciously carried out by users (as they actively need to operate a device), the alleged surveillance of conversations does not involve users taking an action that endangers their privacy (apart from the initial purchase and setup of the device). For this reason and to know whether existing findings can be transferred to this new field, specific research is necessary.

3.2 Smart Device Privacy Concerns

Over the last years, the topic of privacy concerns and smart devices has seen some research, most of it of a qualitative nature. An important aspect found in most studies was that privacy concerns are among the most important factors determining the usage of devices. Emami-Naeini et al. (2019) conducted interviews and found that privacy and security were among the most important factors when deciding whether to purchase an Internet of Things (IoT) device such as a smart speaker. Another study that looked at factors influencing the intention of users to continue using "intelligent personal assistants" (IPA) found security and privacy risks to be important factors that influence the decision to continue using IPAs (Han and Yang, 2018). An interview study by Abdi et al. (2019) on the security and privacy perception concerning Smart Home Personal Assistants found that listening in was an important fear that the participants in their study had and that some even turned their devices off before sleeping or having private conversations. These concerns regarding unwanted surveillance by smart devices was in line with findings from another interview study (Siddike et al., 2018).

These findings show that a) users are generally aware of the topic in connection to these devices and b) the topic can influence decisions such as (continued) usage intention. However, while these studies brought to light valuable insights into privacy concerns surrounding smart devices, they showed that users were afraid of being listened to but not where this perception originated. Also, most of these studies were based on small samples. To precisely examine the factors influencing the perception that devices listen in on users, a larger sample is needed. In this regard, a research-in-progress paper proposed a promising approach and planned on conducting a quantitative study (Saffarizadeh et al., 2017). However, no follow-up paper has been published. The present article thus aims to address the issues mentioned above and to identify the factors that influence privacy concerns regarding smart devices.

4. Model Development

Drawing from the theoretical background to measure the impact of various factors on the PSoC, we developed the surveillance effect model depicted in Figure 1. The model is grounded on acknowledged theories considering influencing factors such as, for example, security (Lee et al., 2020), privacy (Dinev et al., 2013) and trust (Kehr et al., 2015; Malhotra et al., 2004). Lee et al. (2019) investigated Amazon Alexa in the context of users' perception of group harmony. Dinev et al. (2013) developed a theoretical framework for information privacy issues in the Web 2.0. Malhotra et al. (2004) examined humans' behavioral intention in the context of internet users' information privacy concerns and the impact of trusting beliefs and behavioral intention. Finally, Kehr et al. (2015) analyzed institutional trust in the context of smartphone applications and its relation to information disclosure.

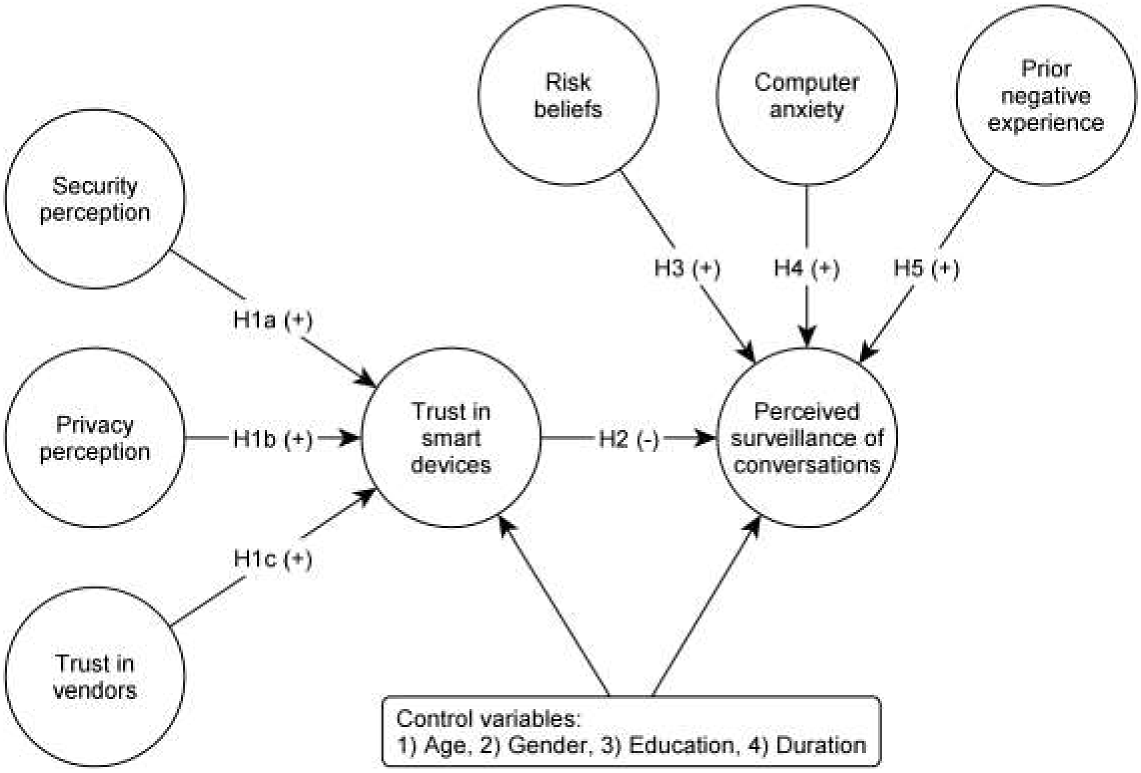

Figure 1: Surveillance effect model including constructs and hypotheses as developed from the literature

Security perception is explained as *“subjective probability with which consumers believe that their private information will not be viewed, stored, and manipulated during transit and storage by inappropriate parties in a manner consistent with their confident expectations”* (Pavlou, 2001). Security perception has recently moved into the center of attention as incidents unveiled that smart devices can be activated by voice commands in TV ads or news programs (Hackett, 2017; Maheshwari, 2017). This goes in line with current research of Zhang et al. (2018) who found that voice-based remote attacks are perceived as highly realistic by individuals. Furthermore, home burglary and counterfeit shopping orders using Amazon Alexa are possible (Lei et al., 2017). Perceived security has been found to positively influence the willingness to share personal information (Dinev and Hart, 2006), and studies show that individuals fear smart devices listen in (Abdi et al., 2019; Siddike and Kohda, 2018). Low security perception influences trusting negatively (Eastlick et al., 2006; Kim et al., 2010; Kim, 2008) and may lead to the refusal to interact with devices (Ba et al., 2003; Gefen et al., 2003). Smart devices are operated using natural language in an open space, and the virtual assistant, running on the cloud-based vendor’s server, is able to control the users’ e-commerce accounts or in-house smart devices (Lee et al., 2020). In this context, security perception is a relevant factor for trust in smart devices. We thus propose:

H1a: Security perception is positively related to trust in smart devices.

Regarding the collection, dissemination and utilization of sensitive information by organizations, people's privacy perception is of great relevance. Privacy perception is the individual's belief in their own ability to handle the disclosure and distribution of personal data (Stone et al., 1983) and is considered as significant predictor of privacy concerns (Xu, 2007; Xu et al., 2011). Culnan (1993) studied attitudes towards personal data that is collected by a supermarket to generate targets for direct-mail solicitations. The results indicate that customers are more concerned about privacy if they assume that they do not have control over their personal data. These concerns can be decreased by putting customers in charge of the initial collection and distribution of their private data (Phelps et al., 2000). Bandyopadhyay (2011) confirmed these findings in the context of consumers in the Indian online market and was further verified across different contexts. Visiting a website entails the risk of discarding the regulation of personal data which leads to greater privacy concerns (Xu et al., 2011). In the context of social media, the users' perception of how much control they have over who is able to obtain their personal data and profiles, has a negative effect on privacy concerns (Nemec Zlatolas et al., 2015). Xu et al. (2008) have found that privacy control strongly influences privacy concerns in online shopping, social media, finance and health-related settings. In general, if individuals perceive of being in charge when exchanging data with organizations, they are more likely to accept the collection of information (Olivero and Lunt, 2004) and consider their privacy safeguarded when they think that they have control of how personal information is used (Anić et al., 2018). Furthermore, research provides evidence that trust is a relevant factor in privacy-related contexts (Malhotra et al., 2004) and important when interacting with technology (Jain and Mishra, 2015; Liao et al., 2011; Miyazaki and Fernandez, 2000). In the context of smart devices, speech interaction poses a risk to the user's privacy by revealing personal information which might be used by third parties to, for example, identify the user, gain access to their systems, or simply process data by pretending to be the user (Chung et al., 2017; Nguyen et al., 2015). We thus argue that privacy perception affects trust in smart devices and hypothesize:

H1b: Privacy perception is positively related to trust in smart devices.

When users request services from websites, apps or social media platforms, they assume that the provider of the service will take responsibility for their personal data (Okazaki et al., 2009). Therefore, trust in the organization providing the service is required. If Internet users trust a company's website, it positively influences their current information disclosure to the website (Metzger, 2006). Peoples' concern for online privacy also decreases trust in commercial websites (Metzger, 2006). If consumers trust the competence, benevolence and integrity of an e-commerce website, it positively affects the willingness to trust the vendor (Fuller et al., 2007). Regarding social media platforms, if a user trusts the platform and believes that disclosing personal information is free of risk, the user is willing to share more information (Dhami et al., 2013). With trust as a key antecedent to online information exchange (Metzger, 2006) and based on the former results, people with lower trust in vendors might be less trusting about their personal information when using smart devices. On the specific subject of smart devices, Lau et al. (2018) found that non-users distrust the vendors of smart speakers. Another study by Abdi et al. (2019) regarding trust concerns showed that individuals fear that their smart device listens to conversations and that it was turned off before going to bed or having private conversations. This goes in line with earlier research of Siddike and Kohda (2018) who identified trust as key factor regarding unwanted surveillance and the intention to use smart speakers. Trust in the vendors offering smart devices including their services is thus fundamental for its utilization. We propose that trust in vendors is affecting trust in smart devices and therefore hypothesize:

H1c: Trust in vendors is positively related to trust in smart devices.

IS research has frequently dealt with trust in individuals or in organizations (e.g., vendors) (Butler, 1991; Jones et al., 1975; Mayer et al., 1995; Rempel et al., 1985; Scanzoni, 1979). 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 will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other part"* (Mayer et al., 1995). Dinev and Hart (2006) measured Internet trust in the context of e-commerce transactions and found trust to be an important factor to disclose personal information when using the Internet. Krasnova et al. (2012) further dealt with institutional trust regarding data-collection on social networking sites and indicate that trust can be understood as tendency to have confidence towards the data-collection technology (Kehr et al., 2015). However, trust in individuals or organizations differs from trust in technology and is more difficult to achieve (Lankton et al., 2015). McKnight et al. (2011) explain trust in an artefact as specific technology possessing required characteristics to perform in a situation with potential negative outcomes. Research found that trust in technology (e.g., smart devices) highly affects usage intentions and is further related to the user's behavior (Bandura, 1986; Bansal and Zahedi, 2015; Davis, 1989; Yan et al., 2013). We therefore argue that trust in smart devices is a relevant factor influencing the PSoC. More specifically, less trust in smart devices might be related to the assumption that the system collects and analyzes private audio data in order to deliver personalized ads, leading to the following hypothesis:

H2: Trust in smart devices is negatively related to the perceived surveillance of conversations.

Risk beliefs may also play a role, as users can associate a potential for loss with disclosing personal information (Dowling and Staelin, 1994). It is expected that risk averse users are less tolerant towards privacy leaks in an online context. Individuals with a high degree of information privacy concerns tend to have lower trusting and risk beliefs (Malhotra et al., 2004). Pan and Zinkhan (2006) have found that consumers with high risk beliefs tend not to trust online merchants that they will deal adequately with private consumer data. A study that focused on strategies to reduce consumers' risk beliefs in Internet shopping has shown a relationship between risk beliefs and the willingness to purchase products online (Jiuan Tan, 1999). Consumers tend to perceive online shopping as a risky activity and only those who are less risk averse are more likely to shop in e-stores. Since these studies only investigate risk beliefs in association with perceived risks in online shops, there is a research gap considering risk beliefs related to online privacy concerns. People that try to avoid risks in their daily lives might be more concerned and careful towards personal data that is collected and stored by organizations, similar to how they feel about e-stores. Therefore, individuals with high risk beliefs might also be more concerned than risk tolerant users that their smart devices are listening in on their conversations. We hypothesize:

H3: Risk beliefs are positively related to the perceived surveillance of conversations.

Computer anxiety is defined by Parasuraman and Igbaria (1990) as an aversion towards computerization. Mediated by common privacy concerns, computer anxiety has the potential to impact users' usage intention (Parasuraman and Igbaria, 1990). Prior studies have focused on a connection between computer anxiety and data leak concerns and could show that a potential loss of private information or security could make people feel anxious when using computers (Powell, 2013). This goes in line with Stewart and Segars (2002) who confirmed that computer anxiety predicts information privacy concern well. Another study also found a positive effect between computer anxiety and the level of privacy concern (Škrinjarić et al., 2018). Osatuyi (2015) sees computer anxiety as uncertainties and risks associated with the current digitalization of goods and services and found a positive influence on consumers' concern for information privacy on social media platforms. Someone who fears computerization and is skeptical towards the ongoing digitalization might also be more likely to believe that the automation process leads to mobile devices listening to and recording everything people say. Thus, we hypothesize that:

H4: Computer anxiety is positively related to the perceived surveillance of conversations.

Škrinjarić et al., (2018) show that prior negative experience with personal data of an Internet user or someone in the vicinity positively affects the level of privacy concern. Experiences might be privacy intrusion, data theft or Internet fraud. An earlier study suggested that the more negative experiences consumers have had on the Internet with information disclosure, the more concerned they are about their privacy and the stronger they perceive risks (Okazaki et al., 2009). A single negative experience is enough to increase the individual's privacy concerns even if the user has mostly had positive experiences. We expect users who have already had negative experiences such as privacy violations to be more likely to believe that they are being listened to by their smart devices. They might have experienced a situation where sensitive data was leaked illegally or they are unsatisfied with the way their personal data has been used before, so they are more likely to believe that companies secretly collect as much data as possible about consumers in order to maximize their profit. We derived the following hypotheses:

H5: Prior negative experience is positively related to the perceived surveillance of conversations.

5. Research Design

To test the developed model, a quantitative online questionnaire was used with various items measuring the constructs in the model. The questionnaire was implemented in LimeSurvey and took about 10 minutes to complete. Participants were briefed about the content and purpose of the study and provided with information about the participants' rights and the anonymous collection of data. The study started with an explanation on smart devices and their purpose as well as providing examples on frequently used systems. Afterwards, the participants were asked to answer questions regarding their demographic data followed by questions on the specific constructs. As last question, complemented by an explanation of the PSoC, the participants were asked whether they had heard about this effect before and if they already had perceived it themselves.

Participants were recruited via Prolific, a commercial platform specifically designed to acquire subjects for surveys (Palan and Schitter, 2018), and selected according to certain conditions: Besides the prerequisite for participants to own a smart device themselves, individuals needed to speak English fluently as the survey was presented in the English language.

5.1 Measures

To assess the degree to which the participants believed that their conversations were possibly monitored by one of their devices, the perceived surveillance of conversations served as the dependent variable. As this study is, to our knowledge, the first to examine this effect, five items were self-developed in advance, covering different aspects in the context of the PSoC, such as conversations being recorded, personal data being analyzed by companies and being shown personalized ads online. The items are "*I am concerned that smart devices record conversations to provide personalized advertising* *on websites and social media"*, *"I think there are companies that analyze audio files recorded by smart devices to provide personalized advertising online"*, *"My smart device listens to me and forwards the data to companies to provide personalized advertising on websites and social media", "I worry that my smart device is recording conversations when I talk to my friends",* and finally *"I am concerned that my smart device is capturing information even though I am not actively using it"*. In our study, the scale for the PSoC had a high reliability with Cronbach's $\alpha = .875$.

The independent variables were measured using items that were derived from verified instruments in previous studies. *Security perception* was measured using 4 items by Lee et al. (2019) exploring the impact of Amazon Alexa on users' perception of group harmony. *Privacy perception* was adapted from Dinev et al.'s (2013) framework for information privacy using 3 items. *Trust in vendors* as well as *risk beliefs* were derived from Malhotra et al. (2004) focusing on internet users' information privacy concerns with 5 items each. 3 items to measure *trust in smart devices* were adapted from Kehr et al. (2015) who dealt with general institutional trust in the context of smartphone applications. *Computer anxiety* was measured using 5 items from Stewart and Segars (2002) who examined it as an impact factor regarding information privacy concerns. Finally, 4 items to measure *prior negative experience* were adapted from Okazaki et al. (2009) who determined the implications of consumers' privacy concerns in the field of smartphone ads. All items in the study were slightly rephrased to transfer them into the context of smart devices and measured using a 5-point Likert scale ranging from "strongly disagree" to "strongly agree". In addition, we measured the age, gender, education and duration of smart device usage of participants as control variables on trust in smart devices and PSoC. The sequence of the online study as well as the complete list of all items can be found in the appendix (cf. Table A.1 – A.2).

5.2 Descriptive Statistics

Overall, 280 participants completed the survey. The collected data set was manually verified for anomalies and suspicious responses which lead to exclusion of three participants due to similarities in their answers. The final dataset consisted of N = 277 participants. The participants were between 18 and 66 years old with a mean age of 29.7 (SD = 9.38), 134 of them female (48.4%), 141 male (50.9%) and 2 neither (0.7%). Of the participants, 68 (24.5%) lived in the UK, 59 (21.3%) in Poland, and 22

(7.9%) in Italy. Most of the participants (163 of 280) had an academic degree with 93 (33.6%) Bachelor graduates, 63 (22.7%) Master graduates and 7 (2.5%) doctorates. 110 participants (39.7%) had a high school degree or equivalent and 4 participants (1.4%) had less than a high school diploma. Smartphones are the most-used smart devices (272), followed by smart watches (163), tablets (159) and smart speakers (105) where the majority (73.6%) was using smart devices for more than 5 years. Finally, 139 (50.2%) participants reported already having experienced the phenomenon of PSoC and 138 (48.8%) participants stated that they had never experienced it. 206 (74.4%) participants had already heard about this effect and 71 (25.6%) had never heard of it before. Detailed information on the descriptive statistics can be found in the appendix (c.f. Table A.10 – A.14).

5.3 PLS-SEM Approach

The presented research model was evaluated using partial least square (PLS) structural equation modeling (SEM), an effective approach to estimate construct reliability and validity as well as causal relationships within complex multistage models (Fornell and Bookstein, 1982). PLS-SEM is especially suitable as it delivers robust approximations for the final estimations (Hair et al., 2011). However, PLS depends on a sufficient sample size to achieve acceptable levels of statistical power (Hair et al., 2011). In this research, the rule of thumb was followed that the number of samples should at least be the number of constructs multiplied by ten (Chin, 1998; Hair et al., 2011; Marcoulides et al., 2009). The calculation was performed using SmartPLS (v. 3.2.8) (Ringle et al., 2015) and jamovi (v. 1.1.8.0) for descriptive statistics. All construct indicators in the model are reflective measurements since they are assumed to be caused by the latent variables (Churchill, 1979). The PLS algorithm was applied using a path weighting scheme with 300 iterations with 10^{-7} as the stop criterion. Bootstrapping was done using a two-tailed bias-corrected and accelerated (BCa) confidence interval method with 4,999 subsamples and blindfolding was calculated with an omission distance of 7 (Henseler et al., 2016).

6. Results

As a first step suggested by Hair et al., (2011), we examined the indicator loadings and deleted items with values smaller than 0.70 as reliable items should be above the threshold of 0.708. Slightly weaker indicators should be kept when they contribute to content validity and are relevant on grounds of measurement theory (Hair et al., 2017, 2011). In case of this study, this only applies to the construct of computer anxiety. Internal consistency was evaluated using Cronbach's alpha, composite reliability and Rho_A where all values are greater than 0.70, indicating satisfying results (Diamantopoulos et al., 2012; Dijkstra and Henseler, 2015; Drolet and Morrison, 2001; Hair et al., 2019). Convergent validity was assessed by measuring the average variance extracted (AVE). The values are greater than 0.50, i.e., at least half the variance of the construct's items is explained (Fornell and Larcker, 1981; Hair et al., 2019; Henseler et al., 2016). The Fornell-Larcker criterion (Fornell and Larcker, 1981) and Heterotrait-monotrait (HTMT) ratio (Henseler et al., 2016) were used to assess the discriminant validity. For the Fornell-Larcker criterion, validity can be assumed as the square root of AVE is greater than any inter-factor correlation (Fornell and Larcker, 1981). Regarding HTMT, validity was present since the values are below 0.90 (Franke and Sarstedt, 2019; Henseler et al., 2016). To alleviate concerns about common method bias (CMB), Harman's one-factor test was conducted for a full collinearity assessment approach. The variance inflation factors (VIF) were lower than the suggested maximum of 3.30 (Kock, 2015). Finally, the cross-loadings were observed to ensure that indicators are not incorrectly assigned to factors (Henseler et al., 2016).

The statistical tests are considered as significant when their p values are lower than or equal to 0.05 and t statistics greater than 1.96 (Greenland et al., 2016). Cohen's f^2 gives the statistical relevance, where effect sizes are considered small, $.02 < f^2 \leq .15$; medium, $.15 < f^2 \leq .35$; or large, $f^2 > .35$ (Cohen, 1988). The exploratory power of the model is measured by R^2. Values range between 0 and 1, where higher values indicate a stronger effect (Hair et al., 2011; Reinartz et al., 2009). However, values should be interpreted in the context of the conducted research, as even lower values for the exploratory power might reveal insights regarding the research model (Hair et al., 2019). For predicting the relevance how well the data can be reproduced by the PLS model, blindfolding was performed using the Stone-Geisser Q^2 measure (Geisser, 1974; Stone, 1974). Predictive accuracy is illustrated by Q^2 values greater than zero, where values higher than 0, 0.25 and 0.5 are considered as small, medium and large effect sizes (Hair et al., 2019) . The goodness of fit (GoF) is assessed using AVE and R^2 (adjusted). The value of

0.59 is above the threshold of 0.36 indicating a valid model (Wetzels et al., 2009). The final results of our evaluation are presented in Figure 2.

We finally conducted a multi-group analysis (Henseler et al., 2009) to compare participants who have not perceived the PSoC (N = 138) and those who already experienced the effect themselves (N = 139). We performed a partial least squares multi-group analysis (PLS-MGA) to assess statistical differences (Henseler et al., 2009). All hypotheses (H1a-c, H2-5) were evaluated for each group separately, and additionally, we tested for significant differences between the two groups in the parameter estimates. Significant differences of path coefficients are indicated by p values below 0.05 or above 0.95 (Henseler et al., 2009). However, the same set of hypotheses as in the overall dataset was significant in each subgroup and there were no significant differences between individuals who had already perceived the effect and those who had not.

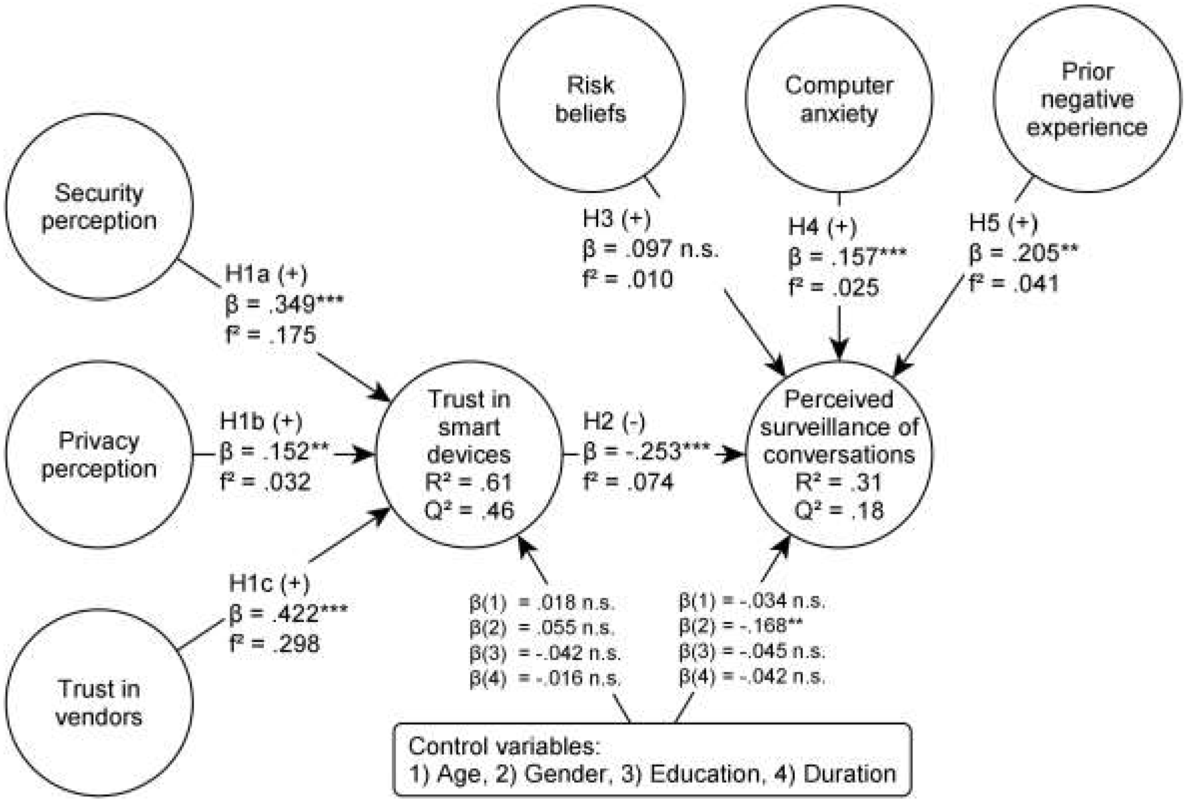

Figure 2: Surveillance effect model with results (N = 277). *p ≤ 0.05; **p≤ 0.01; ***p ≤ 0.001; n.s. = not significant

Overall, the developed surveillance effect model explains 31% of the variance of the PSoC. Additionally, 61% of the variance of trust in smart devices could be explained by our model. We controlled the model using age, gender, education and duration of smart device usage. Security perception, privacy perception, and trust in vendors are significant predictors of trust in smart devices. Regarding the PSoC, trust in smart devices, computer anxiety and prior negative experience are significant where risk beliefs is not. Overall, six of our seven constructs within the research model are substantial, confirming hypotheses H1a, H1b, H1c as well as H2, H4 and H5. Details on the measurement and assessment can be found in the appendix (Tables A.3 – A.9).

7. Discussion

This study identifies a relevant and previously unexplained phenomenon. The vast majority (74.4%) of participants were aware of it, and almost every second participant had experienced it. The perception that conversations are secretly recorded by smart devices is widespread and there is clearly a need for research to explore this phenomenon.

The fear of being surveilled should not be discounted as an urban myth too quickly, as it is a serious problem that is often associated with dystopian scenarios of the future and totalitarian control of institutions and organizations. While the aim of this work is not to find out whether and to what extent people's conversations are actually monitored, this work provides insights into the individual determinants influencing this perception. The results contribute to the understanding of the PSoC phenomenon and its role in society. They also provide an important contribution to research into smart devices.

7.1 Surveillance Effect Model

In the study, the structural equation modeling revealed that six out of seven hypotheses were significant and trust in smart devices, computer anxiety and prior negative experience are the main predictors of the PSoC. Furthermore, a multi-group analysis for comparing participants who had not perceived the surveillance effect and those who had showed no significant differences between the two groups. This indicates that our results hold true regardless of previous exposure.

The impact of security perception, privacy perception and trust in vendors on trust in smart devices goes in line with previous theoretical findings (Chung et al., 2017; Lau et al., 2018; Lee et al., 2020). Smart devices possess unique characteristics which require a high level of trust, they are equipped with microphones and constantly listen to the environment for being able to respond to users' voice commands. In addition, a permanent internet connection is a necessity for executing commands by the virtual assistant, running on the cloud-based vendor's server (Hoy, 2018). As research demonstrated, smart devices are capable of controlling the users' online accounts (Lee et al., 2020) and that third parties might gain access and process data by pretending to be the user (Lau et al., 2018). Thus, security and privacy threats, i.e., wiretapping, compromised devices, malicious voice commands and unintentional voice recording, demand a high level of trust (Chung et al., 2017). This is also indicated by our findings. The safer people feel when interacting with a smart device, the greater the trust in the device itself. Thus, individuals with higher security perception are more likely to share sensitive information. Users who feel that they have enough privacy when using smart devices have more trust towards their device. Therefore, people perceiving sufficient privacy tend to worry less about possible threats. Furthermore, vendors are the main suspects when it comes to the misuse of data as they could benefit financially from using the data. Trust in vendors has been associated with information exchange and various studies have confirmed that a higher trust in vendors increases the eagerness to share personal data (e.g., Dhami et al., 2013; Metzger, 2006). We also reached the same conclusion in our study. The higher the trust in the vendor offering the smart device and its related services, the greater the trust in the system. This indicates that, when individuals perceive that companies are trustworthy in handling personal information, they also feel like the smart device will handle the data carefully. In summary, interacting with smart devices requires revealing sensitive personal information and thus demands high security perception, privacy perception and trust in vendors to establish adequate trust in smart devices.

The results demonstrate that trust in smart devices is not only relevant during interactions between individuals and the system (Chung et al., 2017; Saffarizadeh et al., 2017; Siddike and Kohda, 2018), but also an influencing factor on the perception of being surveilled. It can be stated that higher trust in smart devices lowers the PSoC. Previous research explained that trust in technology is a significant predictor for the continuous use of that technology (Yan et al., 2013), and this condition also applies to the utilization of smart devices. In the context of the PsoC, where people believe that conversations are recorded and analyzed to tailor personalized ads, the effect is influenced by users' trust in the smart device. We thus understand that lower trust in smart devices might result in the feeling of being surveilled.

The findings furthermore show that computer anxiety has a positive effect on PsoC. People with a higher computer anxiety (i.e., those with a tendency to feel uncomfortable around computers) also tend to perceive a larger degree of surveillance on their conversations. This is in line with prior findings that computer anxiety negatively influences the usage behavior (Featherman and Pavlou, 2003), and drives people to remain in their familiar environment. It indicates that people with a general tendency to be more skeptical or uncomfortable around technology are accordingly also more skeptical regarding smart devices and more likely to perceive said effect. These people may actively search for explanations of their discomfort, such as being surveilled. In turn, people with a higher level of computer anxiety might feel uncertainties and risks about the ongoing digitalization. These individuals are more concerned about their private data in general and have a negative attitude towards digitalization and smart devices (Osatuyi 2015).

Also, prior negative experience contributes to the perception of being monitored. This is in line with former research which has shown that consumers who have already had negative experiences on the Internet are more to favor strict regulatory controls in mobile advertising (Okazaki et al., 2009). Individuals are generally more sensitive if they have already experienced harmful practices. In turn, previous negative experience might lead individuals to overthink how their data is processed by service providers. These findings point out the importance of technology companies to carefully handle personal data as not to scare away future users. A bad experience with a company may be enough to increase the skepticism regarding technological applications in general. Accordingly, to not impede possible future use of its services, providers of soft- and hardware alike are responsible to design their services in a way that respects the user's privacy, giving them the confidence that they are in control. This could explain that the effect is perceived stronger by people who have already had bad experiences. In other words, people who have experienced other examples of questionable behavior are more likely to expect companies to violate their privacy to make a profit.

Surprisingly, risk beliefs had no significant impact on the PSoC. Risk tolerant and risk averse people do not appear to differ significantly in their perception that smart devices listen to conversations and transmit these recordings to companies for personalizing online ads. While former research found that individuals with higher risk beliefs tend to avoid disclosing personal information (Dowling and Staelin, 1994) we could not replicate these findings for smart devices. One explanation may be that smart devices are constantly listening in without individuals noticing the difference between capturing information and not capturing information. Consequently, people may not have the feeling of actively disclosing personal information to their smart device, explaining why this factor is not significant in the context of the PSoC.

7.2 Limitations and Future Research

Although we conducted a cross-national survey, the focus of this study did neither lie on the participant's nationality nor on the cultural differences. People in other countries may perceive the surveillance effect differently, for example, when strong data protection laws apply, and government institutions enjoy a high degree of trust. Possible differences in the PSoC depending on the cultural context should be addressed by future research. This is also supported by Xu et al. (2011) who stated that domain-specific privacy concerns may constantly change and thus demand greater attention. News articles about people's experiences with the phenomenon and the results of this research suggest that the PSoC is especially common in a social media context. Also, with computer anxiety and prior negative experience as important predictors of the PSoC, future research could focus on people's past experiences and their influence on the perception of devices secretly listening in. Furthermore, although we carefully evaluated and selected instruments to validate the constructs within the research model, there may be differences between smart devices collecting information when they are not being actively used and their deliberate use to order products or services online. Future research may take into account differing users' perceptions depending on the respective domain.Furthermore, the confirmed hypotheses might also be related and influence each other. Higher computer anxiety could be a result of a user's prior negative experiences. Individuals may tend to build up even more fears, e.g., based on previously experienced data misuse or the loss of private information (Powell, 2013). In addition, increased computer anxiety might be influenced by the level of privacy perception and further, there could be connection between prior negative experience and privacy perception (Škrinjarić et al., 2018). Individuals with prior negative experiences and less privacy perception might tend towards higher computer anxiety. Therefore, further research should take a closer look on the interdependencies of the constructs as well as moderation effects on the PSoC.

Even though we were able to identify relevant factors influencing the PSoC, such as trust in smart devices, computer anxiety and prior negative experience, the developed surveillance effect model only explains 31% of the variance. We thus propose to examine additional predictors of the PSoC in future research. For example, the perceived sensitivity of the content of a conversation might enhance the perception of being monitored by smart devices. In addition, certain personality traits, for instance, openness, extraversion, and neuroticism, might be related to the PSoC since these attributes are closely linked to the perception of specific privacy issues and infringements in an online context (Škrinjarić et al., 2018).

While this study focused on potential variables influencing the PSoC, research on online privacy concern has investigated both antecedents and consequences (I.-D. Anic et al., 2019; Yun et al., 2014), and this might also be a next step for future research on the surveillance effect. It should be investigated if higher levels of PSoC lead to a change in people's behavior and attitudes. For organizations selling smart devices or providing online services it is important to understand the behavior of the consumers. If the perception and concern that conversations or ambient sound are recorded for marketing purposes leads to a decreased willingness to buy and make use of certain products and services, companies might have to act to counter this perception. Some consequences of using smart devices have already been reported. Future research could therefore study the consequences of PSoC, such as a reduced willingness to share private data, the adoption of different technologies including apps, social media and online services and its effects on attitudes towards companies and data protection in general. The newly defined phenomenon of PSoC offers plenty of room for new research ideas.

REFERENCES

Abdi, N., London, C., Ramokapane, K.M., Such, J.M., London, C., Clara, S., 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants This paper is included in the Proceedings of the, in: Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security. pp. 451–466.

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., Wetzels, M., 2015. Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. J. Retail. https://doi.org/10.1016/j.jretai.2014.09.005

Andrejevic, M., Burdon, M., 2015. Defining the Sensor Society. Telev. New Media 16, 19–36. https://doi.org/10.1177/1527476414541552

Anic, I.-D., Budak, J., Rajh, E., Recher, V., Skare, V., Skrinjaric, B., 2019. Extended model of online privacy concern: what drives consumers’ decisions? Online Inf. Rev. 43, 799–817. https://doi.org/10.1108/OIR-10-2017-0281

Anic, I.D., Škare, V., Kursan Milaković, I., 2019. The determinants and effects of online privacy concerns in the context of e-commerce. Electron. Commer. Res. Appl. 36. https://doi.org/10.1016/j.elerap.2019.100868

Ba, S., Whinston, A.B., Zhang, H., 2003. Building trust in online auction markets through an economic incentive mechanism. Decis. Support Syst. 35, 273–286. https://doi.org/10.1016/S0167-9236(02)00074-X

Bandura, A., 1986. Social foundations of thought and action: A social cognitive theory. Prentice-Hall.

Bandyopadhyay, S., 2011. Online Privacy Concerns Of Indian Consumers. Int. Bus. Econ. Res. J. 10. https://doi.org/10.19030/iber.v10i2.1797

Bansal, G., Zahedi, F.M., 2015. Trust violation and repair: The information privacy perspective. Decis. Support Syst. 71, 62–77. https://doi.org/10.1016/j.dss.2015.01.009

Bansal, G., Zahedi, F.M., Gefen, D., 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decis. Support Syst. 49, 138–150. https://doi.org/10.1016/j.dss.2010.01.010

BBC, 2017. Is your phone listening in? Your stories [WWW Document]. URL https://www.bbc.com/news/technology-41802282 (accessed 12.21.20).

Bergström, A., 2015. Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. Comput. Human Behav. 53, 419–426. https://doi.org/https://doi.org/10.1016/j.chb.2015.07.025

Bleier, A., Eisenbeiss, M., 2015. The Importance of Trust for Personalized Online Advertising. J. Retail. 91, 390–409. https://doi.org/10.1016/j.jretai.2015.04.001

Brachten, F., Brünker, F., Frick, N.R.J., Ross, B., Stieglitz, S., 2020. On the ability of virtual agents to decrease cognitive load: an experimental study. Inf. Syst. E-bus. Manag. 18, 187–207. https://doi.org/10.1007/s10257-020-00471-7

Butler, J.K.J., 1991. Toward Understanding and Measuring Conditions of Trust: Evolution of a Conditions of Trust Inventory. J. Manage. 17, 643–663. https://doi.org/10.1177/014920639101700307

CBS, 2018. Are smartphones listening and targeting us with ads? [WWW Document]. URL https://www.cbsnews.com/news/phone-listening-facebook-google-ads/ (accessed 12.21.20).

Chin, W.W., 1998. Methodology for business and management. Modern methods for business research, in: The Partial Least Squares Approach to Structural Equation Modeling. Lawrence Erlbaum Associates Publishers, pp. 295–336.

Chung, H., Iorga, M., Voas, J., Lee, S., 2017. Alexa, Can i Trust You? Computer (Long. Beach. Calif). 50, 100–104. https://doi.org/10.1109/MC.2017.3571053

Churchill, G.A., 1979. A Paradigm for Developing Better Measures of Marketing Constructs. J. Mark. Res. 16, 64–73. https://doi.org/10.2307/3150876

Cohen, J., 1988. Statistical Power Analysis for the Behavioral Sciences, Second Edi. ed. Lawrence Erlbaum Associates.

Culnan, M.J., 1993. “How Did They Get My Name?”: An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. MIS Q. 17, 341. https://doi.org/10.2307/249775

Davis, F.D., 1989. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Q. 13, 319. https://doi.org/10.2307/249008

Dhami, A., Agarwal, N., Chakraborty, T.K., Singh, B.P., Minj, J., 2013. Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook, in: 2013 3rd IEEE International Advance Computing Conference (IACC). IEEE, pp. 465–469. https://doi.org/10.1109/IAdCC.2013.6514270

Di Martino, B., Li, K.-C., Yang, L.T., Esposito, A., 2018. Internet of Everything, Internet of Things. Springer Singapore, Singapore. https://doi.org/10.1007/978-981-10-5861-5

Diamantopoulos, A., Sarstedt, M., Fuchs, C., Wilczynski, P., Kaiser, S., 2012. Guidelines for choosing between multi-item and single-item scales for construct measurement: a predictive validity perspective. J. Acad. Mark. Sci. 40, 434–449. https://doi.org/10.1007/s11747-011-0300-3

Dijkstra, T.K., Henseler, J., 2015. Consistent partial least squares path modeling. MIS Q. 29, 297–316. https://doi.org/10.25300/MISQ/2015/39.2.02

Dinev, T., Hart, P., 2006. An Extended Privacy Calculus Model for E-Commerce Transactions. Inf. Syst. Res. 17, 61–80. https://doi.org/10.1287/isre.1060.0080

Dinev, T., Xu, H., Smith, J.H., Hart, P., 2013. Information privacy and correlates: An empirical attempt to bridge and distinguish privacyrelated concepts. Eur. J. Inf. Syst. 22, 295–316. https://doi.org/10.1057/ejis.2012.23

Dowling, G.R., Staelin, R., 1994. A Model of Perceived Risk and Intended Risk-Handling Activity. J. Consum. Res. 21, 119. https://doi.org/10.1086/209386

Driver, J., 2001. A selective review of selective attention research from the past century. Br. J. Psychol. 92, 53–78. https://doi.org/10.1348/000712601162103

Drolet, A.L., Morrison, D.G., 2001. Do We Really Need Multiple-Item Measures in Service Research? J. Serv. Res. 3, 196–204. https://doi.org/10.1177/109467050133001

Eastlick, M., Lotz, S., Warrington, P., 2006. Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. J. Bus. Res. 59, 877–886. https://doi.org/10.1016/j.jbusres.2006.02.006

Emami-Naeini, P., Dixon, H., Agarwal, Y., Cranor, L.F., 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior, in: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19. ACM Press, New York, New York, USA, pp. 1–12. https://doi.org/10.1145/3290605.3300764

Facebook Inc., 2016. Facebook Does Not Use Your Phone's Microphone for Ads or News Feed Stories [WWW Document]. URL https://about.fb.com/news/h/facebook-does-not-use-your-phones-microphone-for-ads-or-news-feed-stories/ (accessed 12.21.20).

Featherman, M., Pavlou, P., 2003. Predicting E-Services Adoption: A Perceived Risk Facets Perspective. Int. J. Hum. Comput. Stud. 59, 451–474. https://doi.org/10.1016/S1071-5819(03)00111-3

Florack, A., Egger, M., Hübner, R., 2020. When products compete for consumers attention: How selective attention affects preferences. J. Bus. Res. 111, 117–127. https://doi.org/10.1016/j.jbusres.2019.05.009

Fornell, C., Bookstein, F.L., 1982. Two Structural Equation Models: LISREL and PLS Applied to Consumer Exit-Voice Theory. J. Mark. Res. 19, 440. https://doi.org/10.2307/3151718

Fornell, C., Larcker, D.F., 1981. Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. J. Mark. Res. 18, 39–50. https://doi.org/10.2307/3151312

Franke, G., Sarstedt, M., 2019. Heuristics versus statistics in discriminant validity testing: a comparison of four procedures. Internet Res. 29, 430–447. https://doi.org/10.1108/IntR-12-2017-0515

Fuller, M.A., Serva, M.A., Benamati, J. “Skip,” 2007. Seeing Is Believing: The Transitory Influence of Reputation Information on E-Commerce Trust and Decision Making. Decis. Sci. 38, 675–699. https://doi.org/10.1111/j.1540-5915.2007.00174.x

Gefen, D., Karahanna, E., Straub, D.W., 2003. Trust and TAM in online shopping: an integrated model. MIS Q. 27, 51–90. https://doi.org/10.2307/30036519

Geisser, S., 1974. A predictive approach to the random effects model. Biometrika 61, 101–107. https://doi.org/10.1093/biomet/61.1.101

Gironda, J.T., Korgaonkar, P.K., 2018. iSpy? Tailored versus Invasive Ads and Consumers’ Perceptions of Personalized Advertising. Electron. Commer. Res. Appl. 29, 64–77. https://doi.org/10.1016/j.elerap.2018.03.007

Gray, S., 2017. The Future of Microphones in Connected Devices [WWW Document]. URL https://fpf.org/2017/08/10/future-microphones-connected-devices/ (accessed 12.21.20).

Greenland, S., Senn, S.J., Rothman, K.J., Carlin, J.B., Poole, C., Goodman, S.N., Altman, D.G., 2016. Statistical tests, P values, confidence intervals, and power: a guide to misinterpretations. Eur. J. Epidemiol. 31, 337–350. https://doi.org/10.1007/s10654-016-0149-3

Guynn, J., 2018. Facebook has “no plans” to listen to your conversations (for now), but the creepy stories mount [WWW Document]. URL https://eu.usatoday.com/story/tech/talkingtech/2018/06/23/facebook-has-no-plans-listen-your-conversations-now/726568002/

Hackett, R., 2017. Amazon Echo’s Alexa Went Dollhouse Crazy [WWW Document]. URL http://fortune.com/2017/01/09/amazon-echo-alexa-dollhouse/ (accessed 12.21.20).

Hair, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M., Thiele, K.O., 2017. Mirror, mirror on the wall: a comparative evaluation of composite-based structural equation modeling methods. J. Acad.

Mark. Sci. 45, 616–632. https://doi.org/10.1007/s11747-017-0517-x

Hair, J.F., Ringle, C.M., Sarstedt, M., 2011. PLS-SEM: Indeed a Silver Bullet. J. Mark. Theory Pract. 19, 139–152. https://doi.org/10.2753/MTP1069-6679190202

Hair, J.F., Risher, J.J., Sarstedt, M., Ringle, C.M., 2019. When to use and how to report the results of PLS-SEM. Eur. Bus. Rev. 31, 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Han, S., Yang, H., 2018. Understanding adoption of intelligent personal assistants: A parasocial relationship perspective. Ind. Manag. Data Syst. 118, 618–636. https://doi.org/https://doi.org/10.1108/IMDS-05-2017-0214

Hassan, B., 2018. Aussies convinced their smartphone is spying on them [WWW Document]. URL https://www.finder.com.au/press-release-july-2018-1-in-5-aussies-convinced-their-smartphone-is-spying-on-them (accessed 12.21.20).

Henseler, J., Hubona, G., Ray, P.A., 2016. Using PLS path modeling in new technology research: updated guidelines. Ind. Manag. Data Syst. 116, 2–20. https://doi.org/10.1108/IMDS-09-2015-0382

Henseler, J., Ringle, C.M., Sinkovics, R.R., 2009. The use of partial least squares path modeling in international marketing, in: Sinkovics, R.R., Ghauri, P.N. (Eds.), Advances in International Marketing. Emerald Group Publishing, New York, NY, pp. 277–319. https://doi.org/10.1108/S1474-7979(2009)0000020014

Hill, S., 2017. Is Your Smartphone Listening to Your Conversations? [WWW Document]. URL https://www.digitaltrends.com/mobile/is-your-smartphone-listening-to-your-conversations/ (accessed 12.21.20).

Hoy, M.B., 2018. Alexa, Siri, Cortana, and More: An Introduction to Voice Assistants. Med. Ref. Serv. Q. 37, 81–88. https://doi.org/10.1080/02763869.2018.1404391

Hsu, C.-L., Lin, J.C.-C., 2016. An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. Comput.

Human Behav. 62, 516–527. https://doi.org/10.1016/j.chb.2016.04.023

Jain, T., Mishra, P., 2015. Dimensions of Privacy Concerns amongst Online Buyers in India. Int. J. Online Mark. 5, 53–66. https://doi.org/10.4018/ijom.2015010104

Jiuan Tan, S., 1999. Strategies for reducing consumers' risk aversion in Internet shopping. J. Consum. Mark. 16, 163–180. https://doi.org/10.1108/07363769910260515

Jones, A.P., James, L.R., Bruni, J.R., 1975. Perceived leadership behavior and employee confidence in the leader as moderated by job involvement. J. Appl. Psychol. 60, 146–149. https://doi.org/10.1037/h0076359

Junglas, I.A., Johnson, N.A., Spitzmüller, C., 2008. Personality traits and concern for privacy: an empirical study in the context of location-based services. Eur. J. Inf. Syst. 17, 387–402. https://doi.org/10.1057/ejis.2008.29

KC Online Media, L., 2017. No, Google Isn't Eavesdropping on You for Those Crazy Ads and Predictions [WWW Document]. URL https://www.xda-developers.com/no-google-isnt-eavesdropping-on-you-for-those-crazy-ads-and-predictions/ (accessed 12.21.20).

Kehr, F., Kowatsch, T., Wentzel, D., Fleisch, E., 2015. Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. Inf. Syst. J. 25, 607–635. https://doi.org/10.1111/isj.12062

Kim, C., Tao, W., Shin, N., Kim, K.S., 2010. An empirical study of customers' perceptions of security and trust in e-payment systems. Electron. Commer. Res. Appl. 9, 84–95. https://doi.org/10.1016/j.elerap.2009.04.014

Kim, D., Park, K., Park, Y., Ju, J., Ahn, J.-H., 2018. Alexa, Tell Me More: The Effect of Advertisements on Memory Accuracy from Smart Speakers, in: Proceedings of the Pacific Asia Conference on Information Systems (PACIS).

Kim, D.J., 2008. Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study. J. Manag. Inf. Syst. 24, 13–45.

https://doi.org/10.2753/MIS0742-1222240401

Klayman, J., 1995. Varieties of Confirmation Bias. Psychol. Learn. Motiv. - Adv. Res. Theory 32, 385–418. https://doi.org/10.1016/S0079-7421(08)60315-1

Kleinman, Z., 2016. Is your smartphone listening to you? [WWW Document]. URL https://www.bbc.com/news/technology-35639549 (accessed 12.21.20).

Kock, N., 2015. Common method bias in PLS-SEM: A full collinearity assessment approach. Int. J. E-Collaboration 11, 1–10. https://doi.org/https://doi.org/10.4018/ijec.2015100101

Kohut, T., 2018. The internet is convinced our phones are listening to us. Here's what the experts say [WWW Document]. URL https://globalnews.ca/news/4039276/smart-devices-facebook-listening/ (accessed 12.21.20).

Krasnova, H., Veltri, N.F., Günther, O., 2012. Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture. Bus. Inf. Syst. Eng. 4, 127–135. https://doi.org/10.1007/s12599-012-0216-6

Lankton, N., McKnight, D.H., Tripp, J., 2015. Technology, Humanness, and Trust: Rethinking Trust in Technology. J. Assoc. Inf. Syst. 16, 880–918. https://doi.org/10.17705/1jais.00411

Lau, J., Zimmerman, B., Schaub, F., 2018. Alexa, Are You Listening? Proc. ACM Human-Computer Interact. 2, 1–31. https://doi.org/10.1145/3274371

Lee, K., Lee, K.Y., Sheehan, L., 2020. Hey Alexa! A Magic Spell of Social Glue?: Sharing a Smart Voice Assistant Speaker and Its Impact on Users' Perception of Group Harmony. Inf. Syst. Front. 22, 563–583. https://doi.org/10.1007/s10796-019-09975-1

Lei, X., Tu, G.-H., Liu, A.X., Ali, K., Li, C.-Y., Xie, T., 2017. The Insecurity of Home Digital Voice Assistants -- Amazon Alexa as a Case Study.

Liao, C., Liu, C.C., Chen, K., 2011. Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. Electron. Commer. Res. Appl. 10, 702–

715. https://doi.org/10.1016/j.elerap.2011.07.003

Maheshwari, S., 2017. Burger King 'O.K. Google' Ad Doesn't Seem O.K. With Google [WWW Document]. URL https://www.nytimes.com/2017/04/12/business/burger-king-tv-ad-google-home.html?_r=0 (accessed 12.21.20).

Malhotra, N.K., Kim, S.S., Agarwal, J., 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Inf. Syst. Res. 15, 336–355. https://doi.org/10.1287/isre.1040.0032

Marcoulides, Chin, Saunders, 2009. A Critical Look at Partial Least Squares Modeling. MIS Q. 33, 171–175. https://doi.org/10.2307/20650283

Mathews-Hunt, K., 2016. CookieConsumer: Tracking online behavioural advertising in Australia. Comput. Law Secur. Rev. 32, 55–90. https://doi.org/10.1016/j.clsr.2015.12.006

Mayer, R.C., Davis, J.H., Schoorman, F.D., 1995. An Integrative Model Of Organizational Trust. Acad. Manag. Rev. 20, 709–734. https://doi.org/10.5465/amr.1995.9508080335

McKnight, D., Carter, M., B., T.J., Clay, P., 2011. Trust in a specific technology: An investigation of its components and measures. ACM Trans. Manag. Inf. Syst. 2, 12–32. https://doi.org/10.1145/1985347.1985353

McLean, G., Osei-Frimpong, K., 2019. Hey Alexa … examine the variables influencing the use of artificial intelligent in-home voice assistants. Comput. Human Behav. 99, 28–37. https://doi.org/10.1016/j.chb.2019.05.009

Metzger, M.J., 2006. Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. J. Comput. Commun. 9. https://doi.org/10.1111/j.1083-6101.2004.tb00292.x

Mirbabaie, M., Stieglitz, S., Brünker, F., Hofeditz, L., Ross, B., Frick, N.R.J., 2021. Understanding Collaboration with Virtual Assistants – The Role of Social Identity and the Extended Self. Bus. Inf. Syst. Eng. 63, 21–37. https://doi.org/10.1007/s12599-020-00672-x

Miyazaki, A.D., Fernandez, A., 2000. Internet Privacy and Security: An Examination of Online Retailer Disclosures. J. Public Policy Mark. Vol. 19, 54–61. https://doi.org/10.1509/jppm.19.1.54.16942

Nemec Zlatolas, L., Welzer, T., Heričko, M., Hölbl, M., 2015. Privacy antecedents for SNS self-disclosure: The case of Facebook. Comput. Human Behav. 45, 158–167. https://doi.org/10.1016/j.chb.2014.12.012

Nguyen, A., Yosinski, J., Clune, J., 2015. Deep neural networks are easily fooled: High confidence predictions for unrecognizable images, in: IEEE Conference on Computer Vision and Pattern Recognition (CVPR). pp. 427–436.

Nickerson, R.S., 1998. Confirmation Bias: A Ubiquitous Phenomenon in Many Guises. Rev. Gen. Psychol. 2, 175–220. https://doi.org/10.1037/1089-2680.2.2.175

Okazaki, S., Li, H., Hirose, M., 2009. Consumer Privacy Concerns and Preference for Degree of Regulatory Control: A Study of Mobile Advertising in Japan. J. Advert. 38, 63–77. https://doi.org/https://doi.org/10.2753/JOA0091-3367380405

Olivero, N., Lunt, P., 2004. Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. J. Econ. Psychol. 25, 243–262. https://doi.org/10.1016/S0167-4870(02)00172-1

Orr, D.A., Sanchez, L., 2018. Alexa , did you get that? Determining the evidentiary value of data stored by the Amazon® Echo. Digit. Investig. 24, 72–78. https://doi.org/10.1016/j.diin.2017.12.002

Osatuyi, B., 2015. Personality Traits and Information Privacy Concern on Social Media Platforms. J. Comput. Inf. Syst. 55, 11–19. https://doi.org/10.1080/08874417.2015.11645782

Palan, S., Schitter, C., 2018. Prolific.ac—A subject pool for online experiments. J. Behav. Exp. Financ. 17, 22–27. https://doi.org/10.1016/j.jbef.2017.12.004

Pan, E., Ren, J., Lindorfer, M., Wilson, C., Choffnes, D., 2018. Panoptispy: Characterizing Audio and Video Exfiltration from Android Applications. Proc. Priv. Enhancing Technol. 2018, 33–50. https://doi.org/10.1515/popets-2018-0030

Pan, Y., Zinkhan, G.M., 2006. Exploring the impact of online privacy disclosures on consumer trust. J. Retail. 82, 331–338. https://doi.org/10.1016/j.jretai.2006.08.006

Parasuraman, S., Igbaria, M., 1990. An examination of gender differences in the determinants of computer anxiety and attitudes toward microcomputers among managers. Int. J. Man. Mach. Stud. 32, 327–340. https://doi.org/10.1016/S0020-7373(08)80006-5

Pavlou, P., 2001. Integrating Trust in Electronic Commerce with the Technology Acceptance Model: Model Development and Validation, in: Seventh Americas Conference on Information Systems.

Phelps, J., Nowak, G., Ferrell, E., 2000. Privacy Concerns and Consumer Willingness to Provide Personal Information. J. Public Policy Mark. 19, 27–41. https://doi.org/10.1509/jppm.19.1.27.16941

Powell, A.L., 2013. Computer anxiety: Comparison of research from the 1990s and 2000s. Comput. Human Behav. 29, 2337–2381. https://doi.org/10.1016/j.chb.2013.05.012

Preibusch, S., 2013. Guide to measuring privacy concern: Review of survey and observational instruments. Int. J. Hum. Comput. Stud. 71, 1133–1143. https://doi.org/10.1016/j.ijhcs.2013.09.002

Reinartz, W., Haenlein, M., Henseler, J., 2009. An empirical comparison of the efficacy of covariance-based and variance-based SEM. Int. J. Res. Mark. 26, 332–344. https://doi.org/10.1016/j.ijresmar.2009.08.001

Rempel, J.K., Holmes, J.G., Zanna, M.P., 1985. Trust in close relationships. J. Pers. Soc. Psychol. 49, 95–112. https://doi.org/10.1037/0022-3514.49.1.95

Ringle, C.M., Wende, S., Becker, J.-M.-, 2015. SmartPLS 3.

Ross, B., Brachten, F., Stieglitz, S., Wikström, P., Moon, B., Münch, F., Bruns, A., 2018. Social Bots in a Commercial Context – A Case Study on Soundcloud, in: Twenty-Sixth European Conference on Information Systems.

Saffarizadeh, K., Boodraj, M., Alashoor, T.M., 2017. Conversational Assistants: Investigating Privacy Concerns, Trust, and Self-Disclosure, in: Thirty Eighth International Conference on Information Systems. South Korea.

Scanzoni, J., 1979. Social exchange and behavioral interdependence, in: Social Exchange in Developing Relationships. Academic press, New York.

Siddike, M.A.K., Kohda, Y., 2018. Towards a Framework of Trust Determinants in People and Cognitive Assistants Interactions, in: 51st Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2018.672

Siddike, M.A.K., Spohrer, J., Demirkan, H., Kohda, Y., 2018. People's Interactions with Cognitive Assistants for Enhanced Performances, in: 51st Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2018.205

Škrinjarić, B., Budak, J., Žokalj, M., 2018. The effect of personality traits on online privacy concern. Ekon. Pregl. 69, 106–130. https://doi.org/10.32910/ep.69.2.2

Smith, H.J., Milberg, S.J., Burke, S.J., 1996. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. MIS Q. 20, 167. https://doi.org/10.2307/249477

Statista, 2020. Marktanteile der Hersteller am Absatz von intelligenten Lautsprechern weltweit vom 3. Quartal 2016 bis zum 2. Quartal 2020 [WWW Document]. URL https://de.statista.com/statistik/daten/studie/818999/umfrage/marktanteile-der-hersteller-am-absatz-von-intelligenten-lautsprechern-weltweit/ (accessed 12.21.20).

Statista, 2019. Prognose zum Absatz von intelligenten Lautsprechern weltweit von 2018 bis 2023 [WWW Document]. URL https://de.statista.com/statistik/daten/studie/1079997/umfrage/prognose-zum-absatz-von-intelligenten-lautsprechern-weltweit/ (accessed 12.21.20).

Stevens, C., Bavelier, D., 2012. The role of selective attention on academic foundations: A cognitive neuroscience perspective. Dev. Cogn. Neurosci. 2, 30–48. https://doi.org/10.1016/j.dcn.2011.11.001

Stewart, K.A., Segars, A.H., 2002. An Empirical Examination of the Concern for Information Privacy Instrument. Inf. Syst. Res. 13, 36–49. https://doi.org/10.1287/isre.13.1.36.97

Stone, E.F., Gueutal, H.G., Gardner, D.G., McClure, S., 1983. A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. J. Appl. Psychol. 68, 459–468. https://doi.org/10.1037/0021-9010.68.3.459

Stone, M., 1974. Cross-validatory choice and assessment of statistical predictions. J. R. Stat. Soc. 36, 111–147. https://doi.org/10.1111/j.2517-6161.1974.tb00994.x

Wetzels, Odekerken-Schröder, van Oppen, 2009. Using PLS Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration. MIS Q. 33, 177. https://doi.org/10.2307/20650284

Wu, R., 2018. Alexa, Who Are You — A Brief History of Amazon's Voice Assistant and Beyond [WWW Document]. URL https://medium.com/@catalium/alexa-who-are-you-a-brief-history-of-amazons-voice-assistant-and-beyond-eb0dfce065a5 (accessed 12.21.20).

Xu, H., 2007. The Effects of Self-Construal and Perceived Control on Privacy Concerns, in: Twenty Eighth International Conference on Information Systems.

Xu, H., Dinev, T., Smith, H.J., Hart, P., 2011. Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. J. Assoc. Inf. Syst. https://doi.org/10.1016/j.ancard.2012.03.001

Xu, H., Dinev, T., Smith, H.J., Hart, P., 2008. Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View, in: Proceedings of the International Conference on Information Systems. https://doi.org/citeulike-article-id:5770148

Yan, Z., Dong, Y., Niemi, V., Yu, G., 2013. Exploring trust of mobile applications based on user behaviors: An empirical study. J. Appl. Soc. Psychol. 43, 638–659. https://doi.org/10.1111/j.1559-1816.2013.01044.x

Yun, H., Lee, G., Kim, D.J., 2014. A meta-analytic review of empirical research on online information privacy concerns: Antecedents, outcomes, and moderators, in: Thirthy Fifth International Conference on Information Systems.

Zhang, N., Mi, X., Feng, X., Wang, X., Tian, Y., Qian, F., 2018. Understanding and Mitigating the Security Risks of Voice-Controlled Third-Party Skills on Amazon Alexa and Google Home.

Zhou, T., 2011. The impact of privacy concern on user adoption of location-based services. Ind. Manag. Data Syst. 111, 212–226. https://doi.org/10.1108/02635571111115146

APPENDIX

Table A.1. Sequence of the online study

Group	**Question**	**Type**
	Briefing	
Demographic data	What kind of smart device do you own?	Multiple choice
	For how long have you been using smart devices?	List selection
	What is your highest educational level/degree?	List selection
	How old are you?	Numeric input
	What is your gender?	List selection
	In which country are your currently living?	List selection
Risk beliefs	Please evaluate the following statements with regard to your risk beliefs.	5-point Likert scale (“strongly disagree” to “strongly agree”)
Computer anxiety	Please evaluate the following statements with regard to your computer anxiety.	5-point Likert scale (“strongly disagree” to “strongly agree”)

Prior negative experience	Please evaluate the following statements with regard to your prior experiences.	5-point Likert scale (“strongly disagree” to “strongly agree”)
Security perception	Please evaluate the following statements with regard to your security perception when using smart devices.	5-point Likert scale (“strongly disagree” to “strongly agree”)
Privacy perception	Please evaluate the following statements with regard to your privacy perception when using smart devices.	5-point Likert scale (“strongly disagree” to “strongly agree”)
Trust in vendors	Please evaluate the following statements with regard to your trust in vendors of smart devices.	5-point Likert scale (“strongly disagree” to “strongly agree”)
Trust in smart devices	Please evaluate the following statements with regard to your general trust in smart devices.	5-point Likert scale (“strongly disagree” to “strongly agree”)
Perceived surveillance of conversations	Please evaluate the following statements with regard to your perceived surveillance of conversations.	5-point Likert scale (“strongly disagree” to “strongly agree”)
Surveillance effect	Have you heard about this before the study?	Yes/No
	Have you perceived this yourself before the study?	Yes/No
	If you perceived this effect yourself, please describe briefly in what kind of situation.	Text input
	Debriefing	

Table A.2. M = Mean, SD = Standard deviation, CA = Cronbach’s alpha

No.	Item
Security perception (M = 3.37; SD = 0.840; CA = 0.840; adapted from (Lee et al., 2020))	
SPE001	I would feel secure using my smart device.
SPE002	My smart device is a secure means through which to search sensitive information.
SPE003	I would feel totally safe providing sensitive information about myself over my smart device.
SPE004	Overall, my smart device is a safe technology for my purpose of using the system.
Privacy perception (M = 3.20; SD = 0.909; CA = 0.851; adapted from (Dinev et al., 2013))	

PPE001	I feel I have enough privacy when I use smart devices.
PPE002	I am comfortable with the amount of privacy I have.
PPE003	I think my online privacy is preserved when I use smart devices.
Trust in vendors (M = 2.68; SD = 0.824; CA = 0.879; adapted from (Malhotra et al., 2004))	
TIV001	Companies are trustworthy in handling information.
TIV002	Companies tell the truth and fulfill promises related to information provided by me.
TIV003	I trust that companies keep my best interests in mind when dealing with information.
TIV004	Companies are in general predictable and consistent regarding the usage of information.
TIV005	Companies are always honest with customers when it comes to using information that I provide.
Trust in smart devices (M = 2.99; SD = 0.873; CA = 0.877; adapted from (Kehr et al., 2015))	
TSD001	Smart devices are trustworthy in handling client data.
TSD002	Smart devices tell the truth and fulfill promises related to the information provided by me.
TSD003	Smart devices are always honest with customers when it comes to using the information that I would provide.
Risk beliefs (M = 3.31; SD = 0.766; CA = 0.827; adapted from (Malhotra et al., 2004))	
RBE001	In general, it would be risky to give information to online companies.
RBE002	There would be high potential for loss associated with giving information to online companies.
RBE003	There would be too much uncertainty associated with giving information to online companies.
RBE004	Providing online companies with information would involve many unexpected problems.
Computer anxiety (M = 2.43; SD = 0.776; CA = 0.762; adapted from (Stewart and Segars, 2002))	
CAN001	Computers are a real threat to privacy in this country.
CAN002	Sometimes I am afraid the data processing department will lose my data.
CAN003	I am anxious and concerned about the pace of automation in the world.
CAN004	I am easily frustrated by computerized bills.
CAN005	I am sometimes frustrated by increasing automation in my home.

Prior negative experience (M = 2.96; SD = 0.903; CA = 0.795; adapted from (Okazaki et al., 2009))	
PNE001	I have seen my personal information misused by online companies without my authorization.
PNE002	I feel dissatisfied with my earlier choice to send my personal information to online advertisers.
PNE003	My experience in responding to online advertising is very unsatisfactory.
PNE004	In the past, my decision to send my personal information to online advertisers has not been a wise one.
Perceived surveillance of conversations (M = 3.62; SD = 0.925; CA = 0.875; self-developed)	
PSC001	I am concerned that smart devices record conversations to provide personalized advertising on websites and social media.
PSC002	I think there are companies that analyze audio files recorded by smart devices to provide personalized advertising online.
PSC003	My smart device listens to me and forwards the data to companies to provide personalized advertising on websites and social media.
PSC004	I worry that my smart device is recording conversations when I talk to my friends.
PSC005	I am concerned that my smart device is capturing information even though I am not actively using it.

Table A.3. Reliability and Validity Measurements. CA = Cronbach's alpha, RA = rho_A, CR = composite reliability, AVE = average variance extracted

Construct	CA	RA	CR	AVE
Computer anxiety	0.768	0.786	0.837	0.508
Perceived surveillance of conversations	0.877	0.888	0.910	0.668
Prior negative experience	0.801	0.817	0.870	0.626
Privacy perception	0.851	0.857	0.910	0.770
Risk beliefs	0.828	0.830	0.886	0.660
Security perception	0.841	0.852	0.894	0.678
Trust in smart devices	0.879	0.884	0.925	0.804

Trust in vendors	0.879	0.883	0.912	0.676

Table A.4. Major effects measurements. O = original sample, M = sample mean, SD = standard deviation, t = t statistic, p = p value

Path	**O**	**M**	**SD**	**t**	**p**
Computer anxiety → Perceived surveillance of conversations	0.157	0.165	0.051	3.102	0.002
Prior negative experience → Perceived surveillance of conversations	0.205	0.208	0.061	3.347	0.001
Privacy perception → Trust in smart devices	0.152	0.153	0.057	2.660	0.008
Risk beliefs → Perceived surveillance of conversations	0.097	0.096	0.067	1.451	0.147
Security perception → Trust in smart devices	0.349	0.348	0.055	6.385	0.000
Trust in smart devices → Perceived surveillance of conversations	-0.253	-0.252	0.060	4.251	0.000
Trust in vendors → Trust in smart devices	0.422	0.422	0.049	8.643	0.000

Table A.5. Fornell-Larcker Criterion, (1) computer anxiety, (2) perceived surveillance of conversations, (3) prior negative experience, (4) privacy perception, (5) risk beliefs, (6) security perception, (7) trust in smart devices, (8) trust in vendors

	(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**
(1)	**0.713**							
(2)	0.372	**0.817**						
(3)	0.393	0.385	**0.791**					
(4)	-0.345	-0.470	-0.392	**0.878**				
(5)	0.370	0.345	0.447	-0.399	**0.812**			

(6)	-0.382	-0.338	-0.325	0.626	-0.393	**0.824**		
(7)	-0.287	-0.420	-0.368	0.600	-0.355	0.659	**0.897**	
(8)	-0.159	-0.319	-0.437	0.535	-0.394	0.511	0.680	**0.822**

Table A.6. HTMT, (1) computer anxiety, (2) perceived surveillance of conversations, (3) prior negative experience, (4) privacy perception, (5) risk beliefs, (6) security perception, (7) trust in smart devices, (8) trust in vendors

	(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**
(1)								
(2)	0.397							
(3)	0.472	0.435						
(4)	0.387	0.523	0.475					
(5)	0.437	0.385	0.543	0.469				
(6)	0.454	0.368	0.400	0.739	0.473			
(7)	0.305	0.465	0.441	0.686	0.414	0.758		
(8)	0.204	0.352	0.519	0.614	0.459	0.595	0.771	

Table A.7. Cross-loadings of indicators

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
[CAN001]	**0.676**	0.268	0.244	-0.320	0.290	-0.297	-0.266	-0.170
[CAN002]	**0.686**	0.271	0.343	-0.241	0.375	-0.249	-0.217	-0.140
[CAN003]	**0.832**	0.353	0.353	-0.289	0.277	-0.338	-0.275	-0.189
[CAN004]	**0.643**	0.102	0.186	-0.086	0.157	-0.186	-0.050	0.030
[CAN005]	**0.712**	0.219	0.205	-0.192	0.152	-0.235	-0.094	0.031
[PNE001]	0.308	0.275	**0.725**	-0.326	0.240	-0.271	-0.308	-0.334
[PNE002]	0.337	0.363	**0.845**	-0.323	0.414	-0.269	-0.285	-0.358

[PNE003]	0.298	0.260	**0.768**	-0.294	0.372	-0.286	-0.282	-0.311
[PNE004]	0.300	0.306	**0.821**	-0.300	0.374	-0.210	-0.297	-0.379
[PSC001]	0.266	**0.812**	0.352	-0.406	0.354	-0.241	-0.326	-0.292
[PSC002]	0.236	**0.807**	0.248	-0.275	0.226	-0.199	-0.362	-0.245
[PSC003]	0.226	**0.809**	0.185	-0.266	0.129	-0.120	-0.245	-0.155
[PSC004]	0.390	**0.832**	0.331	-0.421	0.290	-0.397	-0.352	-0.253
[PSC005]	0.358	**0.825**	0.397	-0.487	0.348	-0.348	-0.395	-0.316
[PPE001]	-0.265	-0.407	-0.297	**0.873**	-0.255	0.535	0.479	0.444
[PPE002]	-0.336	-0.399	-0.411	**0.893**	-0.391	0.556	0.517	0.441
[PPE003]	-0.303	-0.428	-0.323	**0.867**	-0.394	0.554	0.575	0.516
[RBE001]	0.286	0.302	0.393	-0.369	**0.850**	-0.374	-0.353	-0.379
[RBE002]	0.327	0.276	0.342	-0.267	**0.800**	-0.251	-0.212	-0.246
[RBE003]	0.242	0.271	0.362	-0.340	**0.817**	-0.314	-0.269	-0.346
[RBE004]	0.348	0.271	0.353	-0.319	**0.779**	-0.334	-0.314	-0.304
[SPE001]	-0.301	-0.271	-0.250	0.460	-0.242	**0.812**	0.527	0.383
[SPE002]	-0.268	-0.306	-0.264	0.542	-0.333	**0.869**	0.610	0.442
[SPE003]	-0.319	-0.225	-0.272	0.517	-0.376	**0.753**	0.455	0.425
[SPE004]	-0.379	-0.304	-0.289	0.545	-0.354	**0.855**	0.563	0.437
[TSD001]	-0.248	-0.414	-0.338	0.597	-0.324	0.658	**0.904**	0.643
[TSD002]	-0.302	-0.357	-0.308	0.521	-0.344	0.549	**0.904**	0.586
[TSD003]	-0.222	-0.355	-0.343	0.489	-0.286	0.557	**0.882**	0.597
[TIV001]	-0.148	-0.291	-0.405	0.490	-0.402	0.483	0.573	**0.862**
[TIV002]	-0.232	-0.272	-0.390	0.482	-0.349	0.434	0.578	**0.848**
[TIV003]	-0.086	-0.222	-0.389	0.433	-0.306	0.442	0.598	**0.847**
[TIV004]	-0.150	-0.245	-0.291	0.383	-0.267	0.365	0.497	**0.716**
[TIV005]	-0.038	-0.283	-0.312	0.406	-0.290	0.369	0.542	**0.828**

Table A.8. Inner variance inflations

Construct	Perceived surveillance of conversations	Trust in smart devices
Computer anxiety	1.422	
Perceived surveillance of conversations		
Prior negative experience	1.480	
Privacy perception		1.854
Risk beliefs	1.389	
Security perception		1.797
Trust in smart devices	1.257	
Trust in vendors		1.544

Table A.9. Results of multi-group analysis. b = path coefficient, t = test statistic, p = p value, * = p ≤ 0.05 or p ≥ 0.95, f² = statistical relevance

	p	**t**	**p**	**f²**
Computer anxiety → Perceived surveillance of conversations				
– among participants who have not perceived the PSoC	0.181	2.320	0.021	0.034
– among participants who have perceived the PSoC	0.200	2.731	0.007	0.037
Difference between groups	-0.019		0.014	
Prior negative experience → Perceived surveillance of conversations				
– among participants who have not perceived the PSoC	0.174	1.921	0.055	0.028
– among participants who have perceived the PSoC	0.197	1.822	0.069	0.038
Difference between groups	-0.024		-0.014	
Privacy perception → Trust in smart devices				
– among participants who have not perceived the PSoC	0.179	2.425	0.016	0.058
– among participants who have perceived the PSoC	0.108	1.172	0.242	0.013
Difference between groups	0.071		-0.226	

Risk beliefs → Perceived surveillance of conversations				
– among participants who have not perceived the PSoC	0.190	2.096	0.037	0.034
– among participants who have perceived the PSoC	0.056	0.594	0.553	0.003
Difference between groups	0.134		-0.516	
Security perception → Trust in smart devices				
– among participants who have not perceived the PSoC	0.392	5.208	0.000	0.285
– among participants who have perceived the PSoC	0.336	3.683	0.000	0.124
Difference between groups	0.056		0.000	
Trust in smart devices → Perceived surveillance of conversations				
– among participants who have not perceived the PSoC	-0.196	2.174	0.030	0.043
– among participants who have perceived the PSoC	-0.230	2.600	0.010	0.064
Difference between groups	0.034		0.020	
Trust in vendors → Trust in smart devices				
– among participants who have not perceived the PSoC	0.409	6.324	0.000	0.043
– among participants who have perceived the PSoC	0.427	5.448	0.000	0.264
Difference between groups	-0.018		0.000	

Table A.10. Descriptive statistics (age)

N	277
Missing	0
Mean	29.7
Median	28
Standard deviation	9.38
Minimum	18
Maximum	66

Table A.11. Descriptive statistics (gender)

Levels	Counts	% of Total	Cumulative %
F	134	48.4 %	48.4 %
M	141	50.9 %	99.3 %
D	2	0.7 %	100.0 %

Table A.12. Descriptive statistics (country)

Levels	Counts	% of Total	Cumulative %
Australia	11	4.0 %	4.0 %
Austria	1	0.4 %	4.3 %
Belgium	3	1.1 %	5.4 %
Canada	1	0.4 %	5.8 %
Czech Republic	4	1.4 %	7.2 %
Estonia	6	2.2 %	9.4 %
Finland	2	0.7 %	10.1 %
France	5	1.8 %	11.9 %
Germany	4	1.4 %	13.4 %
Greece	7	2.5 %	15.9 %
Hungary	9	3.2 %	19.1 %
Iceland	1	0.4 %	19.5 %
Ireland	2	0.7 %	20.2 %
Israel	1	0.4 %	20.6 %
Italy	22	7.9 %	28.5 %
Latvia	1	0.4 %	28.9 %
Mexico	3	1.1 %	30.0 %
Netherlands	7	2.5 %	32.5 %

New Zealand	1	0.4 %	32.9 %
Poland	59	21.3 %	54.2 %
Portugal	18	6.5 %	60.6 %
Slovenia	6	2.2 %	62.8 %
South Africa	8	2.9 %	65.7 %
Spain	18	6.5 %	72.2 %
Sweden	1	0.4 %	72.6 %
Switzerland	1	0.4 %	72.9 %
United Kingdom	68	24.5 %	97.5 %
United States	7	2.5 %	100.0 %

Table A.13. Descriptive statistics (education)

Levels	**Counts**	**% of Total**	**Cumulative %**
Bachelor's degree (e.g., BS, BA)	93	33.6 %	33.6 %
Doctorate (e.g., PhD, EdD)	7	2.5 %	36.1 %
High school degree or equivalent	110	39.7 %	75.8 %
Less than a high school diploma	4	1.4 %	77.3 %
Master's degree (e.g., MA, MS, MEd)	63	22.7 %	100.0 %

Table A.14. Descriptive statistics (duration of usage/years)

Levels	**Counts**	**% of Total**	**Cumulative %**
> 1-2 years	8	2.9 %	2.9 %
> 2-3 years	15	5.4 %	8.3 %
> 3-4 years	15	5.4 %	13.7 %
> 4-5 years	35	12.6 %	26.4 %
> 5 years	204	73.6 %	100.0 %