TESIS DE LA UNIVERSIDAD DE ZARAGOZA
2024
292

Natalia Lavado Nalvaiz

# Trust-building mechanisms to reduce the negative consequences of privacy loss when using smart home speakers

Director/es
Lucia Palacios, Laura
Pérez López, Raúl



ISSN 2254-7606

Prensas de la Universidad
Universidad Zaragoza


Universidad de Zaragoza
Servicio de Publicaciones

ISSN 2254-7606

Universidad Zaragoza
1542

Tesis Doctoral

# TRUST-BUILDING MECHANISMS TO REDUCE THE NEGATIVE CONSEQUENCES OF PRIVACY LOSS WHEN USING SMART HOME SPEAKERS


Autor

Natalia Lavado Nalvaiz

Director/es

Lucia Palacios, Laura
Pérez López, Raúl

**UNIVERSIDAD DE ZARAGOZA**
**Escuela de Doctorado**

Programa de Doctorado en Economía y Gestión de las Organizaciones


2024

Universidad Zaragoza
1542

# Tesis Doctoral

## Trust-building mechanisms to reduce the negative consequences of privacy loss when using smart home speakers


Autor

Natalia Lavado Nalvaiz

Director/es

Laura Lucia Palacios

Raúl Pérez López

Facultad de Economía y Empresa



2024

# *Agradecimientos*

*Esta tesis doctoral no habría sido posible sin el apoyo de muchas personas especiales a las que siempre estaré agradecida y que por tanto merecen las siguientes palabras.*

*En primer lugar, me gustaría reconocer a los profesores Laura Lucia Palacios y Raúl Pérez López, los cuales han sido un importante referente para mí en este trabajo. Su excelente orientación y amabilidad desde el primer día hasta el último, ha sido, sin lugar a dudas, la parte más importante de esta tesis doctoral. Ellos me han apoyado siempre, me han escuchado y me han tenido en cuenta en todo momento. Nunca han dejado de preocuparse por mí, ayudándome y apoyándome con cualquier problema que se me presentara. Gracias por vuestro tiempo y esfuerzo, por enseñarme tantísimo y por creer en mí. Gracias por todo.*

*Un agradecimiento especial a las profesoras Blanca Hernández y María José Vela, así como a todos los profesores y personal de servicios del edificio Lorenzo Normante. Os podría nombrar a todos y me faltarían líneas. Gracias por ser ejemplos a seguir, por estar siempre apoyándome, por vuestra eterna generosidad y sonrisa con el estudiantado. He aprendido muchísimo de todos vosotros, tanto a nivel académico, como a nivel personal. Ha sido todo un honor haber sido alumna vuestra y desde hace ya un tiempo, compañera. Con la mano en el corazón os digo que estaré eternamente agradecida y orgullosa de haber formado parte de la familia Lorenzo Normante.*

*Sobre todo, quiero agradecer el apoyo de mi pareja y su familia, ya que sin su apoyo esta tesis no habría salido adelante. Gracias cariño por estar cada día conmigo ayudándome y dándome todo tu amor para mejorar y superar cada desafío de mi vida.*

*También, quiero expresar mi gratitud a mi madre, a mi padre y a mi abuela, que seguro estarán muy orgullosos de mí y que han hecho de mí quién soy a día de hoy, gracias por inculcarme el ser mejor cada día tanto profesional, como personalmente.*

*Además, quiero dar las gracias a mis amigos, que más que amigos son familia. Gracias por estar acompañándome en cada momento importante de mi vida, por celebrar cada éxito y arrimar vuestro hombro en cada fracaso. Vuestro amor, cariño y compañía es de las cosas más importantes de mi vida.*

*Para finalizar, gracias infinitas a todos los que he nombrado y a todos aquellos que me han ayudado alguna vez en la vida, tanto conocidos, como desconocidos, vuestra generosidad y compasión han iluminado mi camino.*

*A todos vosotros, os dedico esta tesis.*

# INDEX OF CONTENTS

**CHAPTER I. INTRODUCTION ..... 11**
1.1. MOTIVATION ..... 12
1.2. STATE OF THE ART ..... 16
1.2.1. The literature on smart speakers. ..... 16
1.2.2. The literature on information privacy and smart speakers. ..... 18
1.3. RESEARCH OPPORTUNITIES AND THESIS' GOALS ..... 22
1.3.1. Promote personalised services for users ..... 23
1.3.2. Invest in a closer and more human relationship with users ..... 26
1.3.3. Increase transparency and user control related to data collection and use ..... 29
REFERENCES ..... 37
APPENDIX 1 ..... 52

**CHAPTER II. HOW PERSONALISATION CAN IMPROVE ATTITUDE TOWARD INFORMATION COLLECTION BY SMART HOME SPEAKERS ..... 59**
2.1. INTRODUCTION ..... 60
2.2. THEORETICAL FRAMEWORK ..... 62
2.2.1. Personalisation ..... 62
2.2.2. Attitude toward information collection ..... 63
2.2.3. Trust ..... 64
2.3. HYPOTHESES ..... 65
2.3.1. Personalisation, trust and intention to continue to use ..... 65
2.3.2. Moderating effect of trust ..... 69
2.4. METHODOLOGY ..... 71
2.4.1. Descriptive results ..... 72
2.5. RESULTS ..... 72
2.5.1. Common method bias ..... 72
2.5.2. Measurement model validation ..... 73
2.5.3. Hypothesis testing ..... 75
2.6. DISCUSSION ..... 79
2.7. CONCLUSIONS ..... 82
2.7.1. Research contribution ..... 82
2.7.2. Managerial implications ..... 84
2.7.3. Research limitations and future research suggestions ..... 85

REFERENCES ..... 87
APPENDIX 2. ..... 95

**CHAPTER III. CAN THE HUMANISATION OF SMART HOME SPEAKERS IMPROVE USERS' ATTITUDE TOWARD COVERT INFORMATION COLLECTION? ..... 97**
3.1. INTRODUCTION ..... 98
3.2. CONCEPTUAL DEVELOPMENT ..... 100
3.2.1. Humanisation ..... 100
3.2.2. Social presence ..... 102
3.2.3. Attitude toward covert information collection ..... 102
3.2.4. Perceived surveillance ..... 103
3.3. HYPOTHESIS DEVELOPMENT ..... 104
3.4. METHODOLOGY ..... 108
3.4.1. Descriptive results ..... 109
3.5. RESULTS ..... 110
3.5.1. Common method bias ..... 110
3.5.2. Measurement model validation ..... 111
3.5.3. Hypothesis testing ..... 112
3.6. DISCUSSION ..... 115
3.7. CONCLUSION ..... 118
3.7.1. Theoretical implications ..... 118
3.7.2. Managerial implications ..... 119
3.7.3. Research limitations and future research suggestions ..... 120
REFERENCES ..... 122
APPENDIX 3 ..... 128

**CHAPTER IV. NOTICE AND CHOICE AS TRUST-BUILDING MECHANISMS: THE IMPORTANCE OF INFORMATION TRANSPARENCY AND INFORMATION SENSITIVITY ..... 129**
4.1. INTRODUCTION ..... 130
4.2. LITERATURE REVIEW ..... 133
4.2.1. Legal privacy framework ..... 133
4.2.2. Privacy–trust–behavioural intention model ..... 134
4.3. HYPOTHESIS DEVELOPMENT ..... 139
4.3.1. The effects of notice and choice on EPP, trust and behaviour ..... 140
4.3.2. The consequences of Effectiveness of Privacy Policy ..... 141

4.3.3. Moderating variables: information sensitivity and the importance of information transparency ..... 143
4.4. METHODOLOGY ..... 146
4.5. RESULTS ..... 147
4.5.1. Common method bias ..... 147
4.5.2. Measurement model validation ..... 148
4.5.3. Structural results ..... 150
4.6. DISCUSSION ..... 155
4.7. CONCLUSION ..... 157
4.7.1. Theoretical contributions ..... 157
4.7.2. Implications for managers ..... 159
4.7.3. Limitations and future research lines ..... 160
REFERENCES ..... 161
APPENDIX 4 ..... 168

**CHAPTER V. GENERAL DISCUSSION AND CONCLUSIONS ..... 171**
5.1. THEORETICAL IMPLICATIONS ..... 176
5.2. MANAGERIAL IMPLICATIONS ..... 181
5.3. LIMITATION AND FUTURE RESEARCH ..... 183
REFERENCES ..... 187

**RESUMEN ..... 191**
MOTIVACIÓN Y OBJETIVOS ..... 192
ESTUDIOS EMPÍRICOS ..... 198

**CONCLUSIONES ..... 201**
CONTRIBUCIONES TEÓRICAS ..... 202
IMPLICACIONES PRÁCTICAS ..... 205
LIMITACIONES Y FUTURAS LINEAS DE INVESTIGACIÓN ..... 207
REFERENCIAS ..... 210

# INDEX OF TABLES

**CHAPTER I. INTRODUCTION ..... 11**

**Table 1.1** Definition of Privacy ..... 19

**Table 1.2** Doctoral dissertation research gaps and objectives ..... 33

**CHAPTER II. HOW PERSONALISATION CAN IMPROVE ATTITUDE TO INFORMATION COLLECTION BY SMART HOME SPEAKERS ..... 59**

**Table 2.1** Sample characteristics ..... 72

**Table 2.2** Items and measurement model ..... 74

**Table 2.3** Discriminant validity ..... 75

**Table 2.4** Indirect effects ..... 78

**Table 2.5** Results of hypothesis testing ..... 78

**CHAPTER III. CAN THE HUMANISATION OF SMART HOME SPEAKERS IMPROVE USERS' ATTITUDE TOWARD COVERT INFORMATION COLLECTION? ..... 97**

**Table 3.1** Sample characteristics ..... 110

**Table 3.2** Items and measurement model ..... 111

**Table 3.3** Discriminant validity ..... 112

**Table 3.4** Mediating effects ..... 115

**CHAPTER IV. NOTICE AND CHOICE AS TRUST-BUILDING MECHANISMS: THE IMPORTANCE OF INFORMATION TRANSPARENCY AND INFORMATION SENSITIVITY ..... 129**

**Table 4.1** Literature on trust-building strategies ..... 137

**Table 4.2** Sample characteristics ..... 146

**Table 4.3** Items and measurement model ..... 148

**Table 4.4** Discriminant validity ..... 149

**Table 4.5** Structural results ..... 150

**Table 4.6** Analysis of mediation effects notice and choice on trust ..... 151

**Table 4.7** Analysis of mediation effects of notice and choice on intention to continue to use. 152

# INDEX OF FIGURES

**CHAPTER I. INTRODUCTION ..... 11**

**Figure 1.1** Most common activities performed through smart speakers in the United States in 2022 by generation ..... 13

**Figure 1.2** Global Smart Speaker Market ..... 14

**Figure 1.3** Market share of smart home speakers in North America 2023 ..... 14

**CHAPTER II. HOW PERSONALISATION CAN IMPROVE ATTITUDE TO INFORMATION COLLECTION BY SMART HOME SPEAKERS ..... 59**

**Figure 2.1** Theoretical model ..... 70

**Figure 2.2** Results of the structural model ..... 76

**Figure 2.3** Moderating effect of trust ..... 77

**CHAPTER III. CAN THE HUMANISATION OF SMART HOME SPEAKERS IMPROVE USERS' ATTITUDE TOWARD COVERT INFORMATION COLLECTION? ..... 97**

**Figure 3.1** Theoretical model ..... 104

**Figure 3.2** Structural model results ..... 114

**Figure 3.3** Quadratic effect of humanisation on trust ..... 114

**CHAPTER IV. NOTICE AND CHOICE AS TRUST-BUILDING MECHANISMS: THE ROLE OF IMPORTANCE OF INFORMATION TRANSPARENCY AND INFORMATION SENSITIVITY ..... 129**

**Figure 4.1** Theoretical model ..... 139

**Figure 4.2** Moderating effect of Information Sensitivity on the relationship between Choice and EPP ..... 153

**Figure 4.3** Moderating effect of Importance of Information Transparency on the relationship between Notice and EPP ..... 154

**Figure 4.4** Moderating effect of Importance of Information Transparency on the relationship between Notice and Trust ..... 154

# CHAPTER I

## INTRODUCTION

## 1.1. MOTIVATION

Artificial intelligence (AI) has become an important topic for both technology practitioners and interested academics (Mehta et al., 2022; Vaid et al., 2023). This is because AI has the potential to influence both decision-making and user attitudes and behaviours (Mariani et al., 2022). Companies have started to deploy AI-based technologies in their interaction interfaces as part of an attempt to improve user experiences by offering personalised services and product recommendations (Klaus and Zaichowsky, 2021).

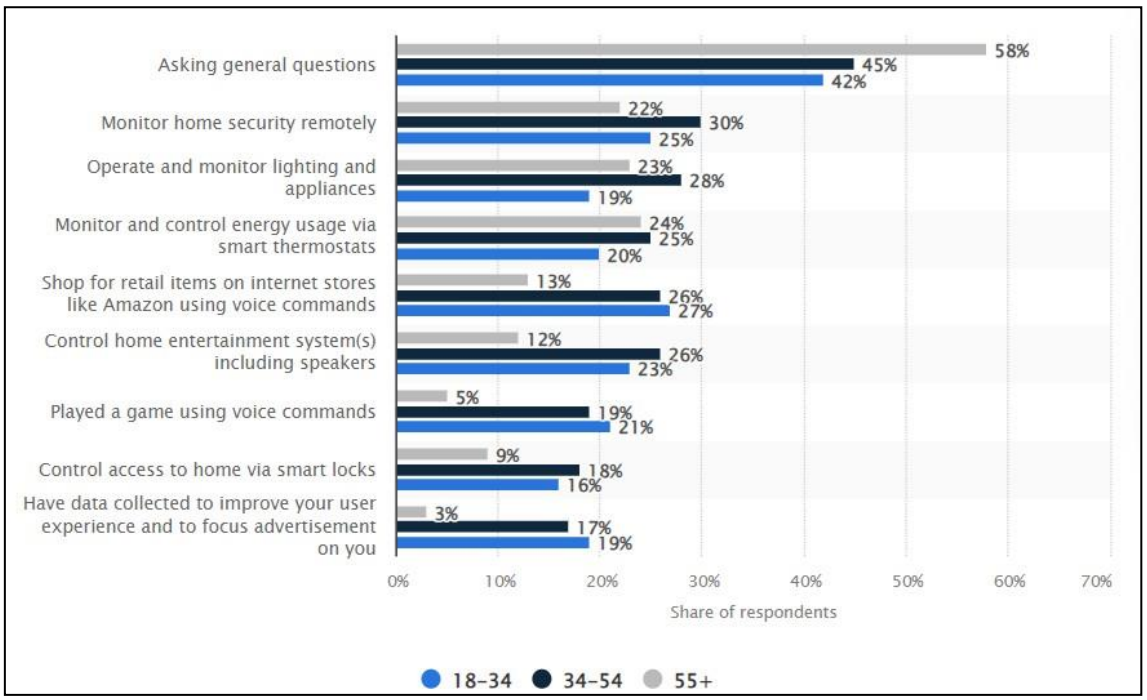
Smart speakers – also called voice assistants – are conversational agents. Users interact with them through voice commands. These devices are characterised by AI capabilities, natural language processing (NLP), and voice recognition capabilities, which have been widely used in recent years (Molinillo et al., 2023; Oliveira et al., 2023). Smart home speakers with embedded AI – such as Google Home, Amazon‘s Alexa, or Apple‘s HomePod – have changed the way people use content, perform everyday tasks, search for information, purchase products, and interact with businesses. Smart home speakers can perform various tasks, including playing music, answering questions, providing weather updates, controlling smart home devices, and shopping online (Bawack et al., 2021; Dey et al., 2019; Hu et a., 2022; Kautish et al., 2023; Mishra et al., 2022; Porcheron et al., 2018).

A Statista study (2023)[1] (Figure 1.1) shows that the most common activities performed through smart speakers in the US during 2022 were asking general questions (e.g., where to have dinner, how to prepare a recipe, or who authored a book), asking for

[1] Statista (2023) https://www.statista.com/statistics/1285045/top-smart-speaker-activities-united-states/#:~:text=In%20a%202022%20survey%20by,to%20shop%20retail%20for%20items

weather forecasts, monitoring home security remotely, and monitoring appliances and lightning.

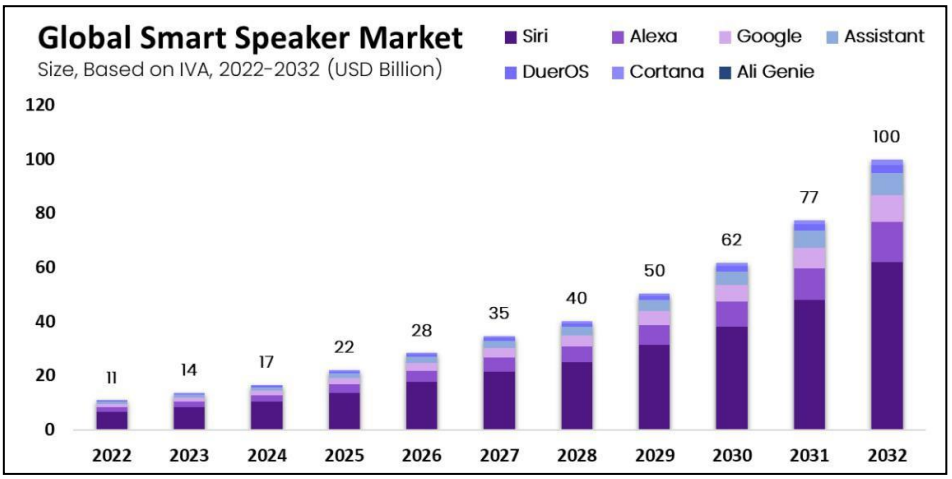
**Figure 1.1** Most common activities performed through smart speakers in the United States in 2022 by generation**.**




*Source: Statista (2023)*

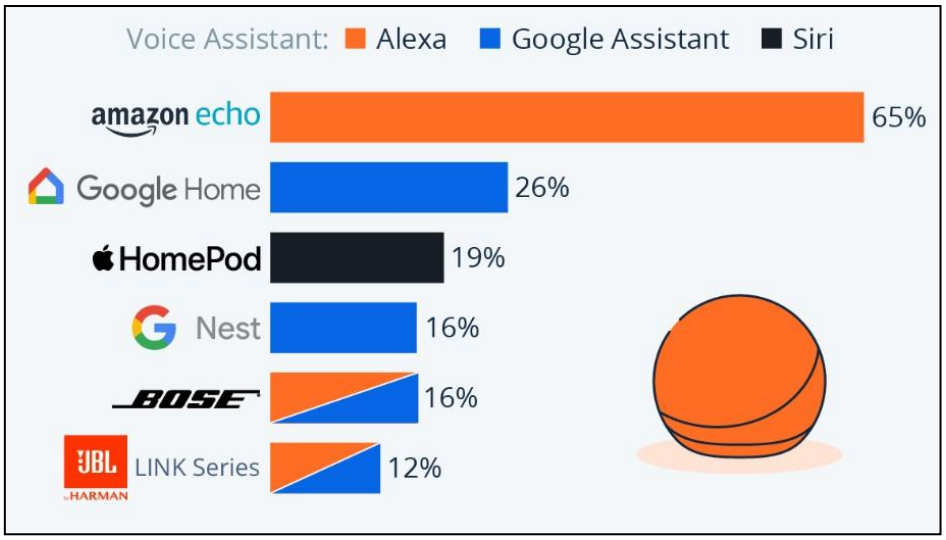
The growth of this type of technology is driving many people to engage with voice assistants as part of their day-to-day lives (Flavián et al., 2022; Go and Sundar, 2019; Klaus and Zaichkowsky, 2021). The smart speaker global market is expected to grow from $11 billion in 2022 to $100 billion by 2032 (Figure 1.2). Looking at regions, North America currently holds 36.40% of the smart speaker market. From 2025 onward, the Asia-Pacific market is expected to overtake North America. According to another Statista study conducted from October 2022 to September 2023, Amazon, which includes Alexa and Echo, is the leading smart speaker brand in the US (with a market share of more than 60%). Google Home and Apple‘s HomePod are the next two most popular choices (owned by 26% and 19% of smart speaker users, respectively) (Figure 1.3).

**Figure 1.2.** Global Smart Speaker Market




*Source: Market.us (2023)*

**Figure 1.3.** Market share of smart home speakers in North America 2023




*Source: Statista (2023)*

With the increased use of smart speakers, users have expressed important privacy concerns, since these devices must collect, store, and share personal information to perform their services (Frick et al., 2021). The relevant privacy concerns might have serious consequences for companies, including direct income loss, risk of litigation, data foreclosure, and increased privacy regulations (Bleier et al., 2020). Company incomes might thus be directly affected because users could refuse to buy from companies that do not respect their privacy (Baruh et al., 2017). Companies that focus

on digital advertising might also lose revenues as users either become reluctant to receive targeted advertisements or use ad-blocking technologies.

Privacy breaches can affect brand value and consequently stock market value. Meta, for example, lost $50,000 million due to a 2018 privacy breach scandal (Checa, 2018). Litigation can also affect revenues when judicial processes result in large fines for companies – an example is the National Data Protection Commission fining Amazon for infringing the European General Data Protection Regulation (Jiménez, 2021). Moreover, if companies are careless with users‘ privacy, then there could be increased motivation to approve regulations that severely limit the collection and management of user data (Bleier et al., 2020).

From an academic perspective, the Marketing Science Institute (2022–2024) has highlighted the importance of studying (a) whether virtual assistants (or chatbots) could augment or replace conventional services, and (b) how they will affect customer experiences. This is in line with academic literature calling for the study of different channels and contexts through which customers relate to companies (De Keyser et al., 2020; Gahler et al., 2023). Studying the use of AI is also strategically aligned with the Ministry of Science and Innovation‘s Spanish State Plan for Scientific, Technical and Innovation Research (2021–2023). This plan established user privacy concerns as a research priority from 2022 to 2024, and it could hamper the advancement of AI technologies and their ostensible benefits.

## 1.2. STATE OF THE ART

### 1.2.1. The literature on smart speakers

Also referred to as voice-activated smart home speakers, virtual assistant speakers, smart home speakers, or voice assistants, smart home speakers are wireless devices that are equipped with voice recognition, machine learning, data mining, and NLP technologies (Hossain et al., 2019; Khan et al., 2020). Smart home speakers utilise AI algorithms to (a) continuously improve their performance and accuracy over time and (b) offer personalised conversations based on previously gathered information. Voice recognition technology enables the device to accurately capture and interpret spoken commands, while NLP allows it to ‗understand' and respond to user requests conversationally (Hossain et al., 2019; Khan et al., 2020).

The literature on smart home speakers has grown considerably and encompasses a wide range of studies (e.g., Aw et al., 2022; Al-Ameen et al., 2021; Bawack et al., 2020; Flavián et al., 2022; Hernández-Ortega and Ferreira, 2021; Klaus and Zaichowsky, 2021; McLean and Osei-Frimpong, 2019; Molinillo et al., 2023; Moriuchi, 2021; Oliveira et al., 2023; Posuhneh, 2021; Shin et al., 2018). Appendix 1.1 provides an overview of these studies' main findings (Appendix 1).

Some studies have found that smart home speakers offer users utilitarian or hedonic benefits (Ashfaq et al., 2021; Mishra et al, 2022). Convenience and efficiency represent utilitarian benefits because smart home speakers can provide information that helps users perform tasks faster and more effectively (Oliveira et al., 2023). These devices collect information from user interactions and feedback. Their integrated AI algorithms then analyse user preferences, behaviours, and historical data to provide personalised assistance and recommendations (Candao et al., 2023; Gao and Liu, 2022).

This enables smart home speakers to offer tailored content, suggestions, and reminders based on individual user profiles (Bernal et al., 2021).

The use of smart home speakers can also offer hedonic benefits (Lucia-Palacios and Pérez-López, 2023; McLean and Frimpong, 2019; Mishra et al., 2022). The relevant emotional experiences primarily involve enjoyment and pleasure. Smart home speakers allow users to entertain themselves by hearing jokes or playing music and games. Hedonic benefits take precedence over utilitarian benefits in the post-usage stage (Gupta et al., 2021; Lee et al., 2020).

Previous research has suggested that socio-emotional and relational value is the main driver behind smart home speaker use (Aw et al., 2022; Lee et al., 2020). These devices‘ role can go beyond efficiency and convenience as they come to resemble something like a partner or friend. Aw et al. (2022) and Jain et al. (2022) have suggested that AI voice assistants can develop relationships with users based on natural communication and personalised experiences. These kinds of interactions are called parasocial relationships.

Some smart home speaker characteristics can affect users‘ attitudes and behaviours. Usefulness, ease of use, and communication skills engender valuable customer experiences (Oliveira et al., 2023). Greater credibility and usefulness can lead users to follow these device‘s recommendations and purchase certain products or services (Flavián et al., 2023). Smart experiences can also build service loyalty by creating greater intimacy and commitment (Hernández-Ortega and Ferreira, 2021).

Intention to continue to use has been explained by utilitarian factors (Saavedra et al., 2023), hedonic factors (Lee et al., 2021), a social presence created by anthropomorphism (Zhou et al., 2023), or by a combination of these factors (Choi and

Drumwright, 2021; McLean and Frimpong 2019; McLean and Osey, 2019). Limayen and Cheung (2011) and Liu and Forsythe (2011) have expressed a need to examine the factors that sustain post-adoption use. This can help us understand the impulse diffusion process. The intention to continue to use is also relevant for managers because it helps to create a habit (Limayem et al., 2007). Habit is a source of inertia among users (Nel and Boshoff, 2019; Shi et al., 2018; Polites and Karahanna, 2012). It can create a preference for using a specific product. Managers are, therefore, incentivised to boost the intention to continue to use as a behavioural outcome.

Despite smart home speakers‘ advantages and functionalities, certain barriers can slow their adoption and diffusion. Some research has identified privacy and data security as significant barriers (Benlian et al., 2019; Lucia-Palacios and Pérez-López, 2023; Maroufkhani et al., 2022; Song et al., 2022). To perform their usual tasks, smart home speakers must constantly listen to their environment, waiting for the words that will activate them (Benlian et al., 2019; Gao and Liu, 2022). Users have, consequently, expressed doubts about the security of their private information.

### 1.2.2. The literature on information privacy and smart speakers

There appears to be no widely agreed definition of ‗privacy‘ in the literature (see Table 1.1). Privacy is studied from different perspectives, leading to definitions of different types of privacy. Some authors claim that privacy is a user‘s right (Van Deg Haag, 1971; Warren and Brandeis, 1890; Westin, 1968), while others view it as a user state or ability (Bélanger and Crossler, 2011; Martin, 2017; Parker, 1974). Some studies define ‗privacy‘ as the control of information or awareness of data practices (Bélanger et al., 2002; Goodwin, 1991; Parker, 1974).

**Table 1.1.** Definition of Privacy

| Author | Concept | Privacy concept |
|---|---|---|
| Warren and Brandeis (1890) | Privacy | The right to be left alone. |
| Westin (1967) | Right to privacy | The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent their data is communicated to others. |
| Van Deg Haag (1971) | Right to privacy | The exclusive access of a person to a realm of their own. The right to privacy entitles one to exclude others from watching, utilising, and invading one‘s private realm. |
| Parker (1974) | Privacy | Control over when and by whom our various parts can be sensed by others. |
| Irwin (1975) | Privacy | The selective control of access to the self or one‘s group. |
| Smith et al. (1996) | Privacy concerns | Operationalised as consumers‘ beliefs, attitudes, and perceptions about their privacy. |
| Smith et al. (1996) | Consumer privacy | Consumer concerns about the use of their revealed information for marketing purposes beyond their intended purpose. |
| Clarke (1999) | Information privacy | The interest someone has in controlling or at least significantly influencing the handling of their personal data. |
| Di Pietro and Mancini (2003) | Privacy | The freedom to not have someone or something interfere in one‘s life without our permission. |
| Malhotra et al. (2004) | Privacy | Individual‘s subjective views about fairness in the information privacy context. |
| Dinev et al. (2006) | Information privacy | A person‘s willingness to render personal information. |
| Nissenbaum (2010) | Privacy | Claim to appropriate flows of personal information within distinctive social contexts. |
| Bélanger and Crossler (2011) | Privacy | One‘s ability to control information about oneself. |
| Smith et al. (2011) | Physical privacy | Physical access to an individual and/or their surroundings and private space. |
| Norberg et al. (2007) | Privacy paradox | The relationship between individuals‘ intentions to disclose personal information and their actual personal information disclosure behaviours. |
| Dinev et al. (2013) | Information privacy | An individual‘s self-assessed state in which external agents have limited access to information about her. |
| Kaminski (2015) | Privacy | Having one‘s own space free from intrusion. |
| Martin (2016) | Privacy | A social contract regarding what, to whom, and for what purpose. |
| Martin et al. (2016) | Privacy as strategy | Using consumer information protection approaches for competitive differentiation. |
| Martin (2017) | Customer data privacy | Customers‘ control over the dissemination and use of their information. |

Given the context of this dissertation, it is adopted the notion of information privacy provided by Dinev et al. (2013). This thesis defines „privacy" as „the individual's self-assessed state in which external agents have limited access to information about them" (Dinev et al., 2013, p. 2999). Thus, privacy refers to a user's assessment of the extent to which external agents (other individuals, organisations, governments, etc.) can access their personal information.

Smart home speakers should start listing and recording after hearing the so-called wake-up word. They can then provide the user with the information they have requested. However, it is not clear to users when the device stops listening or if it „understands" that the conversation has ended. Unless the user manually turns it off, the microphone is always ready to listen to the user's voice. Some research has suggested that there is a common and persistent perception that smart voice assistants are constantly listening (Frick et al., 2021).

Having a smart home assistant disconnected from its microphone frustrates the purpose of voice activation. Some users are, however, concerned about their data being collected and turn the device off before having private conversations. This is supposed to avoid unwanted surveillance (Siddike et al., 2018; Abdi et al., 2019). The perception of surveillance is accentuated when, for example, a user receives messages about a product they have not asked for or that is based on information they have not shared with the device. Involuntary voice activation can lead to an invasion of privacy, interpersonal conflict, and stress (Benlian et al., 2019).

A significant amount of research has been conducted on users' privacy concerns in the context of smart speakers (Abdi et al., 2021; Ammari et al., 2019; Ferraris et al., 2020; Frick et al., 2021; Lim et al., 2022; Lucia-Palacios, Pérez-López, 2021; Malkin et

al., 2019; Shin et al., 2018; Vimalkumar et al., 2021). Appendix 1.2 (Appendix 1) reviews the main studies on privacy and smart home speakers. Ammari et al. (2019) and Malkin et al. (2019) have analysed users‘ concerns about data monitoring. They found that users are concerned about constant surveillance and eavesdropping, but continue to use and purchase smart speakers anyway. Other studies have found that privacy concerns and privacy risks negatively influence smart home speaker adoption (Shin et al., 2018; Yang et al., 2017). Lucia-Palacios and Pérez-López (2021) have argued that smart home speakers‘ autonomy can increase users‘ perception of intrusiveness, which reduces the devices‘ perceived usefulness.

The literature differentiates between two types of information collection according to their transparency: overt or covert (Xu et al., 2011). When information is collected overtly, the company notifies users of the collection. This generates feelings of trust, transparency, and reliability toward the company and control over the provided information (Libaque-Sáenz et al., 2021). When information is collected covertly, users are unaware that the collection is taking place. They have not been explicitly notified (Aguirre et al., 2015; Hayes et al., 2021; Xu et al., 2011). While covert collection might seem unethical, asking for permissions reduces users‘ flow and worsens customer experience (Aguirre et al., 2015).

The debate around personal data collection is a hot topic, one that is at the forefront of information privacy analyses. It is important to recognise which attitude users have toward the strategies used to collect their personal information. If information is collected overtly, then users might have a positive attitude toward the technology. If information is collected covertly, then users might perceive it as an invasion of privacy or surveillance, leading to a negative attitude. This outcome variable has been little studied (Ho et al., 2022). It is, however, a crucial subject because positive

user attitudes toward (overt or covert) data collection will enable companies to deliver personalised messages with or without explicit consent at each interaction.

## 1.3. RESEARCH OPPORTUNITIES AND THESIS' GOALS

Increasing trust in smart home speaker service providers has been put forward as a solution to overcoming privacy, surveillance, and data security concerns. Pitardi and Marriott (2021) have argued that trust is not only related to the intention to use. It is also related to the attitudes or predispositions users have when interacting with voice assistants. Trust in service providers is, then, a key factor influencing human-machine interactions.

The general goal in this dissertation is as follows:

*Study how companies can create trust, reduce the negative consequences of privacy loss due to data collection, and hence boost user intentions to continue to use their smart home speakers.*

This general goal can be divided into more specific goals. The latter revolve around three mechanisms companies can use to create trust and mitigate the negative consequences of data collection:

1. Promote personalised services for users.
2. Invest in a closer and more human relationship with users.
3. Increase transparency and user control related to data collection and use.

In this section, it is suggested how companies can manage these strategies. It also discusses what is known (and not known) about these strategies (based on the literature review).

This dissertation is divided into five chapters. In this introductory chapter, the motivation for the study, the research gaps encountered, and the theoretical context in which this thesis is framed are presented. These are followed by three empirical chapters (Chapters II, III, and IV), which address each of the mechanisms companies can use to create trust, improve user attitudes toward different data collection strategies, and maintain user intentions to continue using their devices. These chapters will focus on developing both a conceptual framework and hypotheses that can lead to quantitatively testing how the relevant mechanisms can improve desirable outcomes. These desirable outcomes include (a) a positive attitude toward data sharing and collection and (b) the intention to continue to use the smart home speakers (see Table 1.2). In these chapters, the methodology, findings, theoretical and practical implications of the empirical studies are explained. Chapter V presents the conclusions of the study, including its limitations and suggestions for future research.

### 1.3.1. Promote personalised services for users (Study 1, Chapter II)

Smart home speakers can provide users with a broad range of benefits, including greater efficiency in task accomplishment and decision-making. They also increase users‘ enjoyment of their daily activities (Klaus and Zaichowsky, 2021; McLean and Osei-Frimpong, 2019; Moriuchi, 2021; Oliveira et al., 2023; Shin et al., 2018). The core of these advantages relies on smart home speakers‘ ability to adapt and optimize their responses to meet user needs through voice commands (Candao et al., 2023; Gao and Liu, 2022). Smart home speakers offer personalised content, suggestions, and reminders

based on individual user profiles (Bernal et al., 2019). This means that they can enhance the value of personalised communication.

According to privacy calculus theory, users rationally evaluate differences between the costs and benefits of sharing information. They then use this calculation as a basis for decision-making (Culnan and Armstrong, 1999; Dinev and Hart, 2006; Xu et al., 2011). Within this calculus, factors like personalisation, utility, or social benefits tend to override the effect of perceived data-sharing risks (Wang et al., 2016).

Numerous studies have analysed the trade-off between personalisation and privacy from the perspective of the so-called personalisation–privacy paradox. Dinev and Hart (2006), Xu et al. (2009), Xu et al. (2011), and Zhu and Chang (2016) consider this paradox to arise from the existence of both psychological and informational decision-making biases (Acquisti et al., 2015). According to Lee et al. (2013), users share personal information (despite their privacy concerns) because they consider both the risk involved and the expected benefit of sharing the information. However, these authors do not take into account how the trade-off affects trust and attitudes toward data collection.

As previously stated, a differentiation can be drawn between overt and covert data collection (Aguirre et al., 2015; Hayes et al., 2021). Previous research has focused on covert data collection to examine users‘ willingness to disclose personal information (Xu et al., 2011). The benefits of personalised messages can outweigh privacy risks when users disclose their personal information. That said, the effect on user attitudes toward covert data collection is unclear. Risks to user privacy (perceived or otherwise) can arise (Xu et al., 2011). Users can feel a sense of invasion, surveillance, loss of privacy, and/or loss of control over their data (Hayes et al., 2021; Kowalczuk 2018).

Further research is required on (a) users‘ attitudes toward how their personal information is collected and (b) the antecedents and consequences of data collection practices on user behaviour.

Given the above, this dissertation asks the following research questions:

- *How can personalised information generate trust and boost the intention to continue to use?*
- *How can personalisation and trust improve users' attitudes toward (overt and covert) data collection?*

In answering these questions, this thesis intends to pursue three research objectives:

Research Objective 1: *Study how personalisation influences user attitudes toward personal data collection (distinguishing between overt and covert collection).*

Research Objective 2: *Determine whether personalised communication (through trust) and user attitudes toward personal data collection (overt and covert) can influence the intention to continue to use.*

Research Objective 3: *Discern whether trust can improve user attitudes toward personal data collection and boost the intention to continue to use.*

Study 1 (Chapter II) represents an attempt to answer these research questions. In doing so, this thesis will employ the theory of privacy calculus and the personalisation–privacy paradox (Aguirre et al. 2015; Dinev and Hart 2006). This represents a theoretical framework for proposing the hypotheses. This thesis will examine the direct

impact of personalisation on trust and user attitudes toward the two pertinent types of data collection: overt and covert. This analysis looks at both direct and indirect effects.

The study also suggests that trust plays a moderating role in the relationship between user attitudes toward covert data collection and intentions to continue to use the device. To do so, a sample of 679 US smart speaker users is employed. Then, SEM analysis was carried out using PLS to test the hypotheses. This study used Preacher and Hayes‘ (2008) methodology to examine the indirect effects of personalisation on the intention to continue to use. The study also includes an analysis of trust‘s moderating/mediating effect. This analysis proceeded according to Hayes‘ (2017) two-step PROCESS.

### 1.3.2. Invest in a closer and more human relationship with users (Study 2, Chapter III)

Previous research on the adoption of voice assistants has shown that these technologies can provide users with socio-emotional and relational values (Aw et al., 2022; Coker and Takhur, 2023; Lee et al., 2020). NLP, voice recognition, machine learning, and data mining have allowed smart home speakers to acquire conversational capabilities similar to those of humans. Characteristics like responsiveness, interactivity, bidirectional communication, and in-context replies are closely related to human communication (Lucia-Palacios and Pérez-López, 2021).

Some research has suggested that users create a personal relationship with the device. This can have positive implications for companies when it comes to (a) brand value, loyalty, and engagement (Hernández-Ortega et al., 2021; Maroufkhani et al., 2022) and (b) the intention to continue to use (Fernandes and Oliveira, 2021). These studies suggest that AI voice assistants can develop parasocial relationships with users

based on natural communication and personalised experiences. Benlian et al. (2019) argue that feelings of familiarity, personal connection, and a social presence created through anthropomorphic design strategies can override sources of anxiety and distrust toward smart home speakers.

Adding anthropomorphic and human features to smart home speakers can influence users‘ emotions, perceptions, and behaviours (Chérif and Lemoine, 2019; Blut et al 2021; Foehr and Gemelman 2020). Three theories appear to be most relevant in the topical literature:

1. Realism maximisation theory (Groom et al., 2009) suggests that a design with human characteristics elicits positive user emotions. It generates a familiar feeling because people can establish a natural and personal connection with a non-human agent (Mende et al., 2019; Toader et al., 2019).
2. Parasocial relationship theory (Horton and Wohl, 1956) suggests that humanisation increases both message credibility (Foehr and Germelmann, 2020; Martin et al., 2020; Poushneh, 2021) and social presence (Chérif and Lemoine, 2019; Kang and Kim, 2022). Humanisation can generate relationships of trust and closeness (even friendship) (Pitardi and Marriott, 2021). It also reduces perceived intrusiveness (Benlian et al., 2019).
3. Uncanny valley theory (Mori et al., 2012) suggests that humanisation has a cubic effect on users‘ emotional responses. Low, but increasing, levels of humanisation can generate affinity toward the device, but there is a point where humanisation starts to be perceived as creepy and disturbing (Mathur et al., 2020). Some research has found that humanisation exerts a quadratic

effect on user behaviour because voice assistants can never be mistaken for a human being (Lavado-Nalvaiz et al., 2022).

As mentioned, covert data collection can give users the perception that they are under surveillance (Benlian et al., 2019; Frick et al., 2021). A brand‘s reputation can be at stake when user trust has been damaged. Humanisation (or anthropomorphism) can potentially help build trust because it generates affinity and increases social presence. That said, it remains unclear whether humanising smart home speakers can mitigate the effects of perceived surveillance and improve user attitudes toward covert data collection.

The following research questions are proposed:

- *How can smart home speaker humanisation improve user attitudes toward covert data collection?*
- *Can smart home speaker humanisation reduce perceptions of surveillance?*

To answer these research questions, this thesis will pursue the following objectives:

Research Objective 4: *Examine how smart home speaker humanisation can both improve user attitudes toward covert data collection and build trust.*

Research Objective 5: *Study how smart home speaker humanisation can reduce perceptions of surveillance.*

Study 2 (Chapter III) is grounded in the three theories mentioned above. The goal is to address the research questions revolving around the role of smart home speaker humanisation during data collection. Following realism maximisation theory, this disseration argues that humanisation can decrease perceived surveillance and

improve user attitudes toward covert data collection (Bavaresco et al., 2020; Lee and Oh, 2019). According to parasocial relationship theory, humanisation helps to create social presence and thus reduce perceptions of surveillance. Uncanny valley theory (Mori et al., 2012) describes the relationship between an object‘s degree of resemblance to a human being and users‘ emotional responses to that object. This theory is useful for exploring humanisation‘s effects on trust.

Study 2, examines trust‘s mediating role, social presence, and user perceptions of surveillance in the relationship between humanisation and attitudes toward covert data collection. In doing so, a survey to 679 US smart home speaker users was carried out. Their responses were analysed using structural equation modelling.

### 1.3.3. Increase transparency and user control related to data collection and use (Study 3, Chapter IV).

Smart home speaker users are often concerned about who is listening. They worry about what information is being collected, when it is being collected, and how it is being used (Manikonda et al., 2018; Vilmalkumar et al., 2021). Users, therefore, often demand control over the collected data; they want to choose if and how their data is collected (Park et al., 2023). Users might also demand an effective privacy policy, one that can reduce perceived privacy risks (Balapour, 2020).

Privacy policies are usually developed according to the US Federal Trade Commission (FTC) and include four dimensions: notice, choice, access, and security. The privacy-trust-behavioural intention model (Liu et al., 2005) defines privacy policy using five dimensions: notice, choice, access, security, and enforcement. Notice and choice are the most visible. They are the only dimensions requiring an active user response.

- Regarding *notice*, a company informs users about their privacy policy and often requires explicit acceptance.
- As for *choice*, consumers must take action to determine their desired level of privacy protection. This is understood to empower users.

Some studies have focused on the presence, readability, and robustness of privacy policies (Aïmeur et al., 2016; Capistrano and Chen, 2015). Some have focused on the content of privacy policies themselves in building trust (Chang et al., 2018; Mutimukwe et al., 2020; Wu et al., 2012). Some have examined how privacy policy statements can be used as trust-building mechanisms in an online environment (Chang et al., 2018; Vila and Kuster, 2011; Wang and Herrando, 2019; Wu et al., 2012). Others have found that consumer awareness of a privacy policy‘s existence can create a sense of psychological comfort (Yang et al., 2020). There is, however, no evidence of privacy policies‘ positive effects (vis-à-vis notice and choice) in the smart home speaker context.

Note that (in the context of this study) the relationship between company and user presents certain asymmetries. While the company possesses a large amount of user data, the user is not always aware of which data is collected and what it is used for. Chang et al. (2018) and Wu et al. (2012) have discussed the importance of providing privacy statements to build user trust. However, these scholars obtained mixed results regarding the effects of notice and choice on user behaviour. Chang et al. (2018) found that only online notices influence perceived effectiveness, while Wu et al. (2012) found that notice is related to user trust, but not choice. There has been little focus in the literature on exploring whether notice and choice have direct impacts on the perceived effectiveness of privacy policy and trust.

Privacy policy importance and usefulness as a trust-building mechanism will depend on individual‘s attitudes toward data collection (Guo et al., 2022; Wu et al., 2012). A personal disposition toward information sensitivity and the importance of information transparency are two important privacy-related factors. They should be taken into account when attempting to explain individual differences related to privacy policy effects (Dinev et al., 2013). Some studies have analysed how a personal disposition toward information sensitivity affects the relationship between privacy risks and personal information disclosures (Hong et al., 2021; Bansal et al., 2016; Kehr et al., 2015; Kim et al., 2019). According to Kim et al. (2019), perceived privacy risks increase with degree of information sensitivity. Users who greatly value their privacy will appreciate the option of consenting to the collection of their personal data.

Dinev et al. define the importance of information transparency as ‒the consumer-rated importance of notifying the consumers what types of information a firm has collected about them, and how that information is going to be used‖ (2013, p.303). Some researchers have focused on companies‘ levels of transparency about their information privacy policies and the resultant effects on information disclosure and trust (Chung et al., 2022; Dehling and Sunyaev, 2023; Hung and Wong, 2009; Karwatzki et al 2017; Walker, 2016). However, user perceptions related to the importance of information transparency have scarcely been analysed. Dinev et al. (2013) and Awad and Krishnan (2006) found that the more importance given to information transparency, the greater the privacy concern. However, little is known about how this attitude can influence the ability of privacy policies to build trust.

Given the above, this thesis asks the following research questions:

- *How can company privacy policy strategies improve trust and enhance the intention to continue to use in the smart home speaker context?*
- *What role do the two personal dispositions – information sensitivity and the importance of information transparency – play when it comes to the impact privacy policy elements have on trust?*

In attempting to answer these questions, this dissertation will pursue the following research objectives:

> Research Objective 6: *Uncover whether notice and choice can (a) improve user perceptions about the effectiveness of privacy policies and trust and (b) enhance the intention to continue to use.*
>
> Research Objective 7: *Analyse the role of information sensitivity and the importance of information transparency in notice's and choice's effects on the effectiveness of privacy policies and trust.*

Study 3 (Chapter IV) applies the privacy-trust-behavioural intention model to address the research questions. On this model, an individual's perception of privacy significantly influences their trust; this trust then affects their behavioural intentions. It is examined whether notice and choice can (a) directly improve privacy policies' effectiveness and user trust in the relevant service provider and (b) indirectly enhance the intention to continue to use.

The moderating role of information sensitivity on the relationship between choice and privacy policy effectiveness will be analysed. Additionally, the information transparency's moderation of the relationship between notice and privacy policy effectiveness will be examined. The methodology used involved SEM analysis using PLS. The sample consisted of 679 US smart home speaker users.

**Table 1.2.** Research gaps and objectives

| Study | Research gaps | Objectives | Theoretical framework | Main concepts |
|---|---|---|---|---|
| **Doctoral thesis** | There is limited research on how companies and developers can implement trust mechanisms to mitigate the privacy and surveillance risks associated with smart home speaker use. | **Main objective:**<br>Study how companies can create trust, reduce the negative consequences of privacy loss due to data collection, and hence boost users‘ intentions to continue using their smart home speakers. | | |
| **Study** | **Research gaps** | **Objectives** | **Theoretical framework** | **Main concepts** |
| **Chapter II, Study 1**<br>How personalisation can improve attitudes toward smart product data collecting. | Prior studies have not analysed the role of trust in user attitudes toward (overt and covert) data collection.<br>Researchers have not examined the antecedents of consumer attitudes toward covert data collection. | **Objective 1:** Analyse how personalising smart home speakers influences user attitudes toward personal data collection (distinguishing between overt and covert types).<br>**Objective 2:** Determine whether communication personalisation through trust and attitudes toward (overt and covert) personal data collection can influence the intention to continue to use.<br>**Objective 3:** Discern whether trust can improve user attitudes toward personal data collection and boost the intention to continue to use. | Privacy calculus theory<br><br>Personalisation–privacy paradox | Overt data collection<br>Covert data collection<br>Personalisation<br>Trust<br>Intention to continue to use |
| **Chapter III, Study 2**<br>Can humanising smart home speakers improve user attitudes toward covert data collection? | Extant studies have not considered (a) which smart home speaker characteristics can reduce perceptions of surveillance and (b) how to improve consumer attitudes toward covert data collection. | **Objective 4:** Examine how smart home speaker humanisation can improve user attitudes toward covert data collection and build trust.<br>**Objective 5**: Study how smart home speaker humanisation can reduce perceptions of surveillance. | Realism maximisation theory<br>Parasocial relationship theory<br>Uncanny valley theory | Humanisation<br>Social presence<br>Surveillance<br>Trust<br>Covert information collection |

**Table 1.2 (continued).** Research gaps and objectives

| Study | Research gaps | Objectives | Theoretical framework | Main concepts |
|---|---|---|---|---|
| **Chapter IV, Study 3**<br>Notice and choice as trust-building strategies: The roles of information sensitivity and importance of information transparency. | Few scholars have examined the effects of notice and choice on trust. Despite the importance of sensitivity and transparency of information, it is not yet clear how they affect privacy policy effectiveness and trust building. | **Objective 6:** Uncover whether notice and choice can improve user perceptions about privacy policy effectiveness, trust, and the intention to continue to use.<br>**Objective 7:** Analyse the role of information sensitivity and the importance of information transparency in notice‘s and choice‘s effects on privacy policy effectiveness and trust. | Privacy-trust-behavioural intention model | Notice<br>Choice<br>Effectiveness of privacy policy<br>Trust<br>Importance of information<br>Transparency<br>Information sensitivity<br>Intention to continue to use |

By addressing the above-mentioned objectives and developing the three studies, we intend to make several contributions. These will be both theoretical and managerial in nature.

*Theoretical perspective*

From a theoretical point of view, this thesis aims to expand existing knowledge related to privacy calculus theory and information management research. This thesis aims to do so by focusing on personalisation‘s effect on trust and user attitudes toward data collection. The dissertation will pay special attention to covert data collection. This strategy is widely employed (Slepchuk and Milne, 2020), but has not received much academic attention.

The dissertation also aims to contribute to existing research on humanisation and social presence. This thesis intends to do so by providing new insights into how these variables can (a) help reduce some of the risks commonly associated with smart home speakers (e.g., the perception of being under surveillance) and (b) enhance and build relationships of trust with service providers.

Another goal relates to furthering the understanding of how privacy policies can generate trust and indirectly affect the intention to continue to use. This thesis will also provide new evidence for the importance of including data-related and individual-specific variables when examining privacy policy effects on user behaviour.

*Managerial perspective*

From a managerial perspective, this dissertation aims to highlight different trust-building mechanisms through which marketers and service providers can (a) improve user attitudes toward data collection and (b) enhance the intention to continue to use

their smart home speakers. A personalised device experience can help create valuable experiences. Users might then exhibit more favourable attitudes toward data collection and increase their use of smart home speakers.

This thesis aims to provide smart home speaker designers and developers with knowledge regarding the appropriate degree of humanisation for these devices. It is suggested that companies should concentrate their efforts on enhancing the design of privacy policies. When doing so, they should remain cognisant of preferences related to information sensitivity and the importance of information transparency.

## REFERENCES


Abdi, N., Zhan, X., Ramokapane, K. M., & Such, J. (2021). Privacy norms for smart home personal assistants. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1-14.

Aguirre, E., Roggeveen, A. L., Grewal, D., & Wetzels, M. (2016). The personalisation-privacy paradox: implications for new media. *Journal of Consumer Marketing*, *33*(2), 98-110.

Aïmeur, E., Lawani, O., & Dalkir, K. (2016). When changing the look of privacy policies affects user trust: An experimental study. *Computers in Human Behavior*, *58*, 368-379.

Al-Ameen MN, Chauhan A, Ahsan MM, & Kocabas H. (2021). Most companies share whatever they can to make money!: comparing user‘s per-ceptions with the data practices of IoT devices. *Proceedings of the International Symposium on Human Aspects of Information Securityand Assurance. Cham: Springer*, 329–340.

Ammari, T., Kaye, J., Tsai, J. Y., & Bentley, F. (2019). Music, search, and IoT: How people (really) use voice assistants. *ACM Transactions on Computer-Human Interaction (TOCHI)*, *26*(3), 1-28.

Ashfaq, M., Yun, J., & Yu, S. (2021). My smart speaker is cool! perceived coolness, perceived values, and users‘ attitude toward smart speakers. *International Journal of Human–Computer Interaction*, *37*(6), 560-573.

Aw, E. C. X., Tan, G. W. H., Cham, T. H., Raman, R., & Ooi, K. B. (2022). Alexa, what's on my shopping list? Transforming customer experience with digital voice assistants. *Technological Forecasting and Social Change*, *180*, 121711.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 13-28.

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management*, *52*, 102063.

Bandara, R., Fernando, M., & Akter, S. (2021). Managing consumer privacy concerns and defensive behaviours in the digital marketplace. *European Journal of Marketing*, *55*(1), 219-246.

Bansal, G., Zahedi, F. M., & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems*, *24*, 624-644.

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26-53.

Bavaresco, R., Silveira, D., Reis, E., Barbosa, J., Righi, R., Costa, C., & Moreira, C. (2020). Conversational agents in business: A systematic literature review and future research directions. *Computer Science Review*, *36*, 100239.

Bawack, R. E., Wamba, S. F., & Carillo, K. D. A. (2021). Exploring the role of personality, trust, and privacy in customer experience performance during voice shopping: Evidence from SEM and fuzzy set qualitative comparative analysis. *International Journal of Information Management*, *58*, 102309.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, 1017-1041.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, *11*(3-4), 245-270.

Benlian, A., Klumpe, J., & Hinz, O. (2020). Mitigating the intrusive effects of smart home assistants by using anthropomorphic design features: A multimethod investigation. *Information Systems Journal*, *30*(6), 1010-1042.

Bernal, G., Montgomery, S. M., & Maes, P. (2021). Brain-computer interfaces, open-source, and democratizing the future of augmented consciousness. *Frontiers in Computer Science*, *3*, 661300.

Bleier, A., & Eisenbeiss, M. (2015). The importance of trust for personalized online advertising. *Journal of Retailing*, *91*(3), 390-409.

Blut, M., Wang, C., Wünderlich, N. V., & Brock, C. (2021). Understanding anthropomorphism in service provision: a meta-analysis of physical robots, chatbots, and other AI. *Journal of the Academy of Marketing Science*, *49*(4), 632-658.

Brause, S. R., & Blank, G. (2023). ‗There are some things that I would never ask Alexa'–privacy work, contextual integrity, and smart speaker assistants. *Information, Communication & Society*, 1-16.

Candao, G. C., Herrando, Carolina, H., & Martín-De, M. J. (2023). Affective Interaction with Technology: The Role of Virtual Assistants in Interactive Marketing, *in Wang, C. (ed.). The Palgrave Handbook of Interactive Marketing*, 275-298

Capistrano, E. P. S., & Chen, J. V. (2015). Information privacy policies: The effects of policy characteristics and online experience. *Computer Standards & Interfaces*, *42*, 24-31.

Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers‘ perceived privacy. *Government Information Quarterly*, *35*(3), 445-459.

Checa, A. A. T. (2018). *Talking about surveillance and human rights: how the Mexican press discussed the Gobierno Espia investigation*.

Chérif, E., & Lemoine, J. F. (2019). Anthropomorphic virtual assistants and the reactions of Internet users: An experiment on the assistant‘s voice. *Recherche et Applications en Marketing (English Edition)*, *34*(1), 28-47.

Cho, G., Choi, J., Kim, H., Hyun, S., & Ryoo, J. (2019). Threat modeling and analysis of voice assistant applications. In *Information Security Applications: 19th International Conference, WISA 2018, Jeju Island, Korea, August 23–25, 2018, Revised Selected Papers 19*, 197-209.

Choi, T. R., & Drumwright, M. E. (2021). ―OK, Google, why do I use you?‖ Motivations, post-consumption evaluations, and perceptions of voice AI assistants. *Telematics and Informatics*, *62*, 101628.

Chung, J., Bleich, M., Wheeler, D. C., Winship, J. M., McDowell, B., Baker, D., & Parsons, P. (2021). Attitudes and perceptions toward voice-operated smart speakers among low-income senior housing residents: comparison of pre-and post-installation surveys. *Gerontology and Geriatric Medicine*, *7*, 23337214211005869.

Chung, W. Y., Nam, J., Ryong, K., & Lee, D. (2022). When, how, and what kind of information should Internet service providers disclose? A study on the transparency that users want. *Telematics and Informatics*, *70*, 101799.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, *42*(2), 60-67.

Coker, K. K., & Thakur, R. (2023). Alexa, may I adopt you? The role of voice assistant empathy and user-perceived risk in customer service delivery. *Journal of Services Marketing*, 0887-6045

Culnan, M. J. (1993). " How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, 341-363.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, *10*(1), 104-115.

De Keyser, A., Verleye, K., Lemon, K. N., Keiningham, T. L., & Klaus, P. (2020). Moving the customer experience field forward: introducing the touchpoints, context, qualities (TCQ) nomenclature. *Journal of Service Research*, *23*(4), 433-455.

Dehling, T., & Sunyaev, A. (2023). A design theory for transparency of information privacy practices. *Information Systems Research*.

Dey, S., & Hossain, A. (2019). Session-key establishment and authentication in a smart home network using public key cryptography. *IEEE Sensors Letters*, *3*(4), 1-4.

Di Pietro, R., & Mancini, L. V. (2003). Security and privacy issues of handheld and wearable wireless devices. *Communications of the ACM*, *46*(9), 74-79.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research*, *17*(1), 61-80.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295-316

Ferraris, D., Bastos, D., Fernandez-Gago, C., & El-Moussa, F. (2021). A trust model for popular smart home devices. *International Journal of Information Security*, *20*(4), 571-587.

Flavián, C., Akdim, K., & Casaló, L. V. (2023). Effects of voice assistant recommendations on consumer behavior. *Psychology & Marketing*, *40*(2), 328-346.

Flavián, C., Pérez-Rueda, A., Belanche, D., & Casaló, L. V. (2022). Intention to use analytical artificial intelligence (AI) in services–the effect of technology readiness and awareness. *Journal of Service Management*, *33*(2), 293-320.

Foehr, J., & Germelmann, C. C. (2020). Alexa, can I trust you? Exploring consumer paths to trust in smart voice-interaction technologies. *Journal of the Association for Consumer Research*, *5*(2), 181-205.

Fox, G., Clohessy, T., van der Werff, L., Rosati, P., & Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behavior*, *121*, 106806.

Frick, N. R., Wilms, K. L., Brachten, F., Hetjens, T., Stieglitz, S., & Ross, B. (2021). The perceived surveillance of conversations through smart devices. *Electronic Commerce Research and Applications*, *47*, 101046.

Gahler, M., Klein, J. F., & Paul, M. (2023). Customer experience: Conceptualization, measurement, and application in omnichannel environments. *Journal of Service Research*, *26*(2), 191-211.

Gao, L., Waechter, K. A., & Bai, X. (2015). Understanding consumers‘ continuance intention toward mobile purchase: A theoretical framework and empirical study–A case of China. *Computers in Human Behavior*, *53*, 249-262.

Go, E., & Sundar, S. S. (2019). Humanizing chatbots: The effects of visual, identity and conversational cues on humanness perceptions. *Computers in Human Behaviour*, *97*, 304-316.

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing*, *10*(1), 149-166.

Groom, V., Nass, C., Chen, T., Nielsen, A., Scarborough, J. K., & Robles, E. (2009). Evaluating the effects of behavioral realism in embodied agents. *International Journal of Human-Computer Studies*, *67*(10), 842-849.

Guo, Y., Wang, X., & Wang, C. (2022). Impact of privacy policy content on perceived effectiveness of privacy policy: the role of vulnerability, benevolence and privacy concern. *Journal of Enterprise Information Management*, *35*(3), 774-795.

Gupta, R., Jain, K., & Jajodia, I. (2021). Determinants of smart speaker adoption intention: extending the theory of planned behaviour. *International Journal of Technology Marketing*, *15*(2-3), 181-202.

Guzman, A. L. (2020). Ontological boundaries between humans and computers and the implications for human-machine communication. *Human-Machine Communication*, *1*, 37-54.

Ha, Q. A., Chen, J. V., Uy, H. U., & Capistrano, E. P. (2021). Exploring the privacy concerns in using intelligent virtual assistants under perspectives of information sensitivity and

anthropomorphism. *International Journal of Human–Computer Interaction*, *37*(6), 512-527.

Han, S., and Yang, H. (2018). Understanding adoption of intelligent personal assistants: A parasocial relationship perspective. *Industrial Management and Data Systems*, *118*(3), 618-636.

Hayes, A. F. (2017). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. Guilford publications.

Hayes, J. L., Brinson, N. H., Bott, G. J., & Moeller, C. M. (2021). The Influence of Consumer–Brand Relationship on the Personalized Advertising Privacy Calculus in Social Media. *Journal of Interactive Marketing*, *55*, 16-30.

Hernandez-Ortega, B., & Ferreira, I. (2021). How smart experiences build service loyalty: The importance of consumer love for smart voice assistants. *Psychology & Marketing*, *38*(7), 1122-1139.

Ho, M. T., Mantello, P., Ghotbi, N., Nguyen, M. H., Nguyen, H. K. T., & Vuong, Q. H. (2022). Rethinking technological acceptance in the age of emotional AI: surveying Gen Z (Zoomer) attitudes toward non-conscious data collection. *Technology in Society*, *70*, 102011.

Hong, A., Nam, C., & Kim, S. (2020). What will be the possible barriers to consumers' adoption of smart home services?. *Telecommunications Policy*, *44*(2), 101867.

Horton, D., & Richard Wohl, R. (1956). Mass communication and para-social interaction: Observations on intimacy at a distance. *Psychiatry*, *19*(3), 215-229.

Hossain, M. S., Muhammad, G., & Alamri, A. (2019). Smart healthcare monitoring: a voice pathology detection paradigm for smart cities. *Multimedia Systems*, *25*, 565-575.

Hsieh, S. H., and Lee, C. T. (2021). Hey Alexa: examining the effect of perceived socialness in usage intentions of AI assistant-enabled smart speaker. *Journal of Research in Interactive Marketing*, *15*(2), 267-294

Hu, P., Lu, Y., & Wang, B. (2022). Experiencing power over AI: The fit effect of perceived power and desire for power on consumers' choice for voice shopping. *Computers in Human Behavior*, *128*, 107091.

Hung, H., & Wong, Y. H. (2009). Information transparency and digital privacy protection: are they mutually exclusive in the provision of e-services?. *Journal of Services Marketing*, *23*(3), 154-164.

Irwin, A., & Martin, C. (1976). Privacy: A Conceptual Analysis. *Environment and Behavior*, *8*(1), 7-29.

Jain, S., Basu, S., Dwivedi, Y. K., & Kaur, S. (2022). Interactive voice assistants. Does brand credibility assuage privacy risks? *Journal of Business Research*, *139*, 701-717.

Jiménez, A., & Oleson, J. C. (2022). The Crimes of Digital Capitalism. *Mitchell Hamline L. Rev.*, *48*, 971.

Kaminski, M. E. (2015). Regulating real-world surveillance. *Washington Law Review*, *90*, 1113.

Kang, H., & Kim, K. J. (2022). Does humanization or machinization make the IoT persuasive? The effects of source orientation and social presence. *Computers in Human Behavior*, *129*, 107152.

Kang, H., & Oh, J. (2023). Communication privacy management for smart speaker use: Integrating the role of privacy self-efficacy and the multidimensional view. *New Media & Society*, *25*(5), 1153-1175.

Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems*, *34*(2), 369-400.

Kautish, P., Purohit, S., Filieri, R., & Dwivedi, Y. K. (2023). Examining the role of consumer motivations to use voice assistants for fashion shopping: The mediating role of awe experience and eWOM. *Technological Forecasting and Social Change*, *190*, 122407.

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. *Information Systems Journal*, *25*(6), 607-635.

Khan, U., Ahmad, M. B., Shafiq, F., & Sarim, M. (2020). Urdu Natural Language Processing Issues and Challenges: A Review Study. In *Intelligent Technologies and Applications: Second International Conference, INTAP 2019, Bahawalpur, Pakistan, November 6–8, 2019, Revised Selected Papers 2* (pp. 461-470). Springer Singapore.

Kim, D., Park, K., Park, Y., & Ahn, J. H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, *92*, 273-281.

Klaus, P., & Zaichkowsky, J. L. (2022). The convenience of shopping via voice AI: Introducing AIDM. *Journal of Retailing and Consumer Services*, *65*, 102490.

Kowalczuk, P. (2018). Consumer acceptance of smart speakers: a mixed methods approach. *Journal of Research in Interactive Marketing*, *12*(4), 418-431.

Krafft, M., Arden, C. M., & Verhoef, P. C. (2017). Permission marketing and privacy concerns—Why do customers (not) grant permissions? *Journal of Interactive Marketing*, *39*, 39-54.

Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on human-computer interaction*, *2*(CSCW), 1-31.

Lavado-Nalvaiz, N., Lucia-Palacios, L., & Pérez-López, R. (2022). The Role of the Humanisation of Smart Home Speakers in the Personalisation–Privacy Paradox. *Electronic Commerce Research and Applications*, 53, 101146.

Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies*, 71(9), 862-877.

Lee, J. M., & Rha, J. Y. (2016). Personalisation–privacy paradox and consumer conflict with the use of location-based mobile commerce. *Computers in Human Behaviour*, *63*, 453-462.

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. *Information Systems Frontiers*, *22*, 563-583.

Lee, S. A., & Oh, H. (2021). Anthropomorphism and its implications for advertising hotel brands. *Journal of Business Research*, *129*, 455-464.

Li, H., Luo, X. R., Zhang, J., & Xu, H. (2017). Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Information & management*, 54(8), 1012-1022.

Libaque-Sáenz, C. F., Wong, S. F., Chang, Y., & Bravo, E. R. (2021). The effect of fair information practices and data collection methods on privacy-related behaviours: A study of mobile apps. *Information & Management*, *58*(1), 103284.

Lim, W. M., Kumar, S., Verma, S., & Chaturvedi, R. (2022). Alexa, what do we know about conversational commerce? Insights from a systematic literature review. *Psychology & Marketing*, *39*(6), 1129-1155.

Limayem, M., Hirt, S. G., & Cheung, C. M. (2007). How habit limits the predictive power of intention: The case of information systems continuance. *MIS Quarterly*, 705-737.

Liu, C., & Forsythe, S. (2011). Examining drivers of online purchase intensity: Moderating role of adoption duration in sustaining post-adoption online shopping. *Journal of retailing and consumer services*, *18*(1), 101-109.

Lucia-Palacios, L., & Pérez-López, R. (2021). Effects of home voice assistants' autonomy on instrusiveness and usefulness: direct, indirect, and moderating effects of interactivity. *Journal of Interactive Marketing*, *56*, 41-54.

Lucia-Palacios, L., & Pérez-López, R. (2023). How can autonomy improve consumer experience when interacting with smart products? *Journal of Research in Interactive Marketing*, *17*(1), 19-37.

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

Maccario, G., & Naldi, M. (2023). Alexa, Is My Data Safe? The (Ir) relevance of Privacy in Smart Speakers Reviews. *International Journal of Human–Computer Interaction*, *39*(6), 1244-1256.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, *15*(4), 336-355.

Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Egelman, S., & Wagner, D. (2019). Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies*, *2019*(4).

Mani, Z., & Chouk, I. (2017). Drivers of consumers‘ resistance to smart products. *Journal of Marketing Management*, *33*(1-2), 76-97.

Manikonda, L., Deotale, A., & Kambhampati, S. (2018, December). What's up with privacy? User preferences and privacy concerns in intelligent personal assistants. In *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*, 229-235.

Mariani, M. M., Hashemi, N., & Wirtz, J. (2023). Artificial intelligence empowered conversational agents: A systematic literature review and research agenda. *Journal of Business Research*, *161*, 113838.

Market.us' report (2023) https://market.us/report/smart-speaker-market/request-sample/ (access 27/12/2023)

Maroufkhani, P., Asadi, S., Ghobakhloo, M., Jannesari, M. T., & Ismail, W. K. W. (2022). How do interactive voice assistants build brands' loyalty? *Technological Forecasting and Social Change*, *183*, 121870.

Martin, B. A., Jin, H. S., Wang, D., Nguyen, H., Zhan, K., & Wang, Y. X. (2020). The influence of consumer anthropomorphism on attitudes toward artificial intelligence trip advisors. *Journal of Hospitality and Tourism Management*, *44*, 108-111.

Martin, K. (2015). Privacy notices as tabula rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online. *Journal of Public Policy & Marketing*, *34*(2), 210-227.

Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics*, *137*, 551-569.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36-58.

Mathur, M. B., Reichling, D. B., Lunardini, F., Geminiani, A., Antonietti, A., Ruijten, P. A., & Szuts, A. (2020). Uncanny but not confusing: Multisite study of perceptual category confusion in the Uncanny Valley. *Computers in Human Behavior*, *103*, 21-30.

McLean, G., & Osei-Frimpong, K. (2019). Hey Alexa… examine the variables influencing the use of artificial intelligent in-home voice assistants. *Computers in Human Behavior*, *99*, 28-37.

Mehta, P., Jebarajakirthy, C., Maseeh, H. I., Anubha, A., Saha, R., & Dhanda, K. (2022). Artificial intelligence in marketing: A meta-analytic review. *Psychology & Marketing*, *39*(11), 2013-2038.

Mende, M. A., Fischer, M. H., & Kühne, K. (2019). The use of social robots and the uncanny valley phenomenon. *AI love you: developments in human-robot intimate relationships*, 41-73.

Mishra, A., Shukla, A., & Sharma, S. K. (2022). Psychological determinants of users‘ adoption and word-of-mouth recommendations of smart voice assistants. *International Journal of Information Management*, *67*, 102413.

Molinillo, S., Rejón-Guardia, F., Anaya-Sánchez, R., & Liébana-Cabanillas, F. (2023). Impact of perceived value on intention to use voice assistants: The moderating effects of personal innovativeness and experience. *Psychology & Marketing*, *40*(11), 2272-2290.

Mols, A., Wang, Y., & Pridmore, J. (2022). Household intelligent personal assistants in the Netherlands: Exploring privacy concerns around surveillance, security, and platforms. *Convergence*, *28*(6), 1841-1860.

Mori, M., MacDorman, K. F., & Kageki, N. (2012). The uncanny valley [from the field]. *IEEE Robotics & Automation Magazine*, *19*(2), 98-100.

Moriuchi, E. (2021). An empirical study on anthropomorphism and engagement with disembodied AIs and consumers' re-use behavior. *Psychology & Marketing*, *38*(1), 21-42.

MSI (2022). Marketing Science Instiurte Research Proprities (2022-2024). https://www.msi.org/wp-content/uploads/2022/10/MSI-2022-24-Research-Priorities-Final.pdf (access 26/12/2023)

Mutimukwe, C., Kolkowska, E., & Grönlund, Å. (2020). Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Government Information Quarterly*, *37*(1), 101413.

Nel, J., & Boshoff, C. (2019). Online customers‘ habit-inertia nexus as a conditional effect of mobile-service experience: A moderated-mediation and moderated serial-mediation investigation of mobile-service use resistance. *Journal of Retailing and Consumer Services*, *47*, 282-292.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32-48.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100-126.

Oliveira, G. G., Lizarelli, F. L., Teixeira, J. G., & de Sousa Mendes, G. H. (2023). Curb your enthusiasm: Examining the customer experience with Alexa and its marketing outcomes. *Journal of Retailing and Consumer Services*, *71*, 103220.

Park, S., Lenhart, A., Zimmer, M., & Vitak, J. (2023). " Nobody's Happy": Design Insights from {Privacy-Conscious} Smart Home Power Users on Enhancing Data Transparency, Visibility, and Control. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*.

Parker, G. A. (1974). Assessment strategy and the evolution of fighting behaviour. *Journal of Theoretical Biology*, *47*(1), 223-243.

Patrizi, M., Šerić, M., & Vernuccio, M. (2024). Hey Google, I trust you! The consequences of brand anthropomorphism in voice-based artificial intelligence contexts. *Journal of Retailing and Consumer Services*, *77*, 103659.

Pitardi, V., & Marriott, H. R. (2021). Alexa, she's not human but… Unveiling the drivers of consumers' trust in voice-based artificial intelligence. *Psychology & Marketing*, *38*(4), 626-642.

Polites, G. L., & Karahanna, E. (2012). Shackled to the status quo: The inhibiting effects of incumbent system habit, switching costs, and inertia on new system acceptance. *MIS Quarterly*, 21-42.

Poushneh, A. (2021). Humanizing voice assistant: The impact of voice assistant personality on consumers‘ attitudes and behaviors. *Journal of Retailing and Consumer Services*, 58, 102283

Preacher, K. J., & Hayes, A. F. (2008). *Assessing mediation in communication research* (pp. 13-54). London: The Sage sourcebook of advanced data analysis methods for communication research.

Saavedra, Á., Chocarro, R., Cortiñas, M., & Rubio, N. (2023). Impact of process and outcome quality on intention for continued use of voice assistants. *Spanish Journal of Marketing-ESIC*.

Shi, X., Lin, Z., Liu, J., & Hui, Y. K. (2018). Consumer loyalty toward smartphone brands: The determining roles of deliberate inertia and cognitive lock-in. *Information & Management*, *55*(7), 866-876.

Shin, J., Park, Y., & Lee, D. (2018). Who will be smart home users? An analysis of adoption and diffusion of smart homes. *Technological Forecasting and Social Change*, *134*, 246-253.

Siddike, M. A. K., Spohrer, J., Demirkan, H., & Kohda, Y. (2018). People‘s interactions with cognitive assistants for enhanced performances. Hawaii International Conference on System Sciences (HICSS-51), https://aisel.aisnet.org/hicss-51/da/smart_service_systems/4/ (access 15/02/2024).

Slepchuk, A. N., & Milne, G. R. (2020). Informing the design of better privacy policies. *Current Opinion in Psychology*, *31*, 89-93.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly*, 989-1015.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 167-196.

Song, M., Du, J., Xing, X., & Mou, J. (2022). Should the chatbot ―save itself‖ or ―be helped by others‖? The influence of service recovery types on consumer perceptions of recovery satisfaction. *Electronic Commerce Research and Applications*, *55*, 101199.

Statista (2023). https://www.statista.com/chart/23943/share-of-us-adults-who-own-smart-speakers/ (access 27/12/2023)

Statista (2023) https://www.statista.com/statistics/1285045/top-smart-speaker-activities-united-states/#:~:text=In%20a%202022%20survey%20by,to%20shop%20retail%20for%20items. (access 27/12/2023)

Taddicken, M. (2013). 13 privacy, surveillance, and self-disclosure in the social web. *Internet and Surveillance: the challenges of Web 2.0 and social media*, *16*, 255-272.

Toader, D. C., Boca, G., Toader, R., Măcelaru, M., Toader, C., Ighian, D., & Rădulescu, A. T. (2019). The effect of social presence and chatbot errors on trust. *Sustainability*, *12*(1), 256.

Vaid, S., Puntoni, S., & Khodr, A. (2023). Artificial intelligence and empirical consumer research: A topic modeling analysis. *Journal of Business Research*, *166*, 114110.

Van Den Haag, E. (2017). On privacy. In *Privacy and Personality* (pp. 149-168). Routledge.

Vila, N., & Kuster, I. (2011). Consumer feelings and behaviours towards well designed websites. *Information & Management*, *48*(4-5), 166-177.

Vimalkumar, M., Sharma, S. K., Singh, J. B., & Dwivedi, Y. K. (2021). ‗Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior*, *120*, 106763.

Walker, K. L. (2016). Surrendering information through the looking glass: Transparency, trust, and protection. *Journal of Public Policy & Marketing*, *35*(1), 144-158.

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, *36*(4), 531-542.

Wang, Y., & Herrando, C. (2019). Does privacy assurance on social commerce sites matter to millennials? *International Journal of Information Management*, *44*, 164-177.

Warren, S. D., & Louis, D. (1890). Brandeis, The Rgkht to Priva. Harvard Law Review, *4*, 193.

Westin, A. F. (1967). Special report: legal safeguards to insure privacy in a computer society. *Communications of the ACM*, *10*(9), 533-537.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, *25*(1), 166.

Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, *28*(3), 889-897.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalisation-privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*(1), 42-52.

Yang, H., Lee, H., & Zo, H. (2017). User acceptance of smart home services: an extension of the theory of planned behavior. *Industrial Management & Data Systems*, *117*(1), 68-89.

Yang, Q., Gong, X., Zhang, K. Z., Liu, H., & Lee, M. K. (2020). Self-disclosure in mobile payment applications: Common and differential effects of personal and proxy control enhancing mechanisms. *International Journal of Information Management*, *52*, 102065.

Yu, L., Li, H., He, W., Wang, F. K., & Jiao, S. (2020). A meta-analysis to explore privacy cognition and information disclosure of internet users. *International Journal of Information Management*, *51*, 102015.

Zhou, P., Xie, Y., & Liang, C. (2023). How to increase consumers‘ continued use intention of artificial intelligence voice assistants? The role of anthropomorphic features. *Electronic Markets*, *33*(1), 60.

Zhu, Y. Q., & Chang, J. H. (2016). The key role of relevance in personalized advertisement: Examining its impact on perceptions of privacy invasion, self-awareness, and continuous use intentions. *Computers in Human Behavior*, *65*, 442-447.

## APPENDIX 1.

**Appendix 1.1.** Voice assistant literature review

| Author/s | Main findings |
|---|---|
| Abdi et al. (2019) | Perceptions about privacy/security issues fall into four categories (built-in skills, third-party skills, smart device management, and shopping). |
| Al-Ameen et al. (2021) | The perception of data collection sharing and protection appears at odds with the data practices stated in manufacturers‘ privacy policies. |
| Ashfaq et al. (2021) | Consumer attitudes toward smart speakers are influenced by functional, hedonic, and economic value rather than social value. |
| Aw et al. (2022) | Parasocial interactions and the perception of smart shopping enhance AI-enabled customer experiences. Perceived security levels significantly influence perceptions of smart shopping. |
| Benlian et al. (2020) | Anthropomorphism mitigates the harmful effects of intrusive technological functions. |
| Brause and Blank (2023) | Even smart speaker assistants users who express indifference about their privacy strive to protect it. |
| Candao et al. (2023) | Digital social interactions are based on three communication tools: text, sound, and image. Virtual assistants‘ anthropomorphic characteristics play a noteworthy role in emotion transmissions. |
| Cho et al. (2019) | Inquiry into the sensitivity of information that can leak through smart speakers. |
| Coker and Takhur (2023) | Perceived empathy toward virtual assistants improves user attitudes toward them. It also boosts virtual assistant adoption and use. |
| Flavián et al. (2023) | Voice-based recommendations are more effective than online consumer reviews when it comes to altering consumer behaviour. Recommendations by males are more effective than those by females. |
| Foehr and Germelmann (2020) | Consumers follow various pathways toward trusting smart technology, one such pathway relates to anthropomorphism. |
| Frick et al. (2021) | Three predictors affect the perceptions about surveillance: trust in smart devices, computer anxiety, and previous negative experiences. |
| Gao and Liu (2022) | AI manifests itself as personalised profiling, navigation, nudges, and retention during various customer journey stages. |
| Gupta et al. (2021) | Trust and ease of use are predictors of attitudes toward smart speaker use. |
| Ha et al. (2021) | The level of device anthropomorphism. |
| Han and Yang (2018) | Interpersonal attraction, security, and privacy influence the choices of intelligent personal assistants. |
| Hernández-Ortega and Ferreira (2021) | Smart voice assistants experiences influence consumers‘ passion for the technology. Passion explains intimacy and commitment, which concurrently leads to service loyalty. |

**Appendix 1.1 (Continued).** Voice assistant literature review

| Author/s | Main findings |
|---|---|
| Ho et al. (2022) | Consumers are not concerned about covert data collection. They have a neutral attitude toward this collection strategy. |
| Hsieh and Lee (2021) | Social cues and parasocial interactions influence trust, perceived usefulness, and ease of use. |
| Jain et al. (2022) | Users in high versus low arousal negative emotion groups have different perceptions of utility gratification. |
| Kang and Oh (2021) | Perceived benefits of CPM theory are positively correlated with privacy disclosure and boundary linking, while perceived privacy risks are negatively correlated with these two strategies. |
| Lau et al. (2018) | The incomplete understanding of privacy risks. |
| Lucia-Palacios and Pérez-López (2021) | Interactivity plays a notable role in reducing intrusiveness and moderating autonomy‘s effect on intrusiveness. |
| Lucia-Palacios and Pérez-López (2023) | Usefulness, interactivity, and _coolness‘ have a positive mediating effect on autonomy and value experiences, while intrusiveness has a negative mediating effect. |
| Lutz and Newlands (2021) | Privacy protection is affected by social presence, pertinent concerns, and utilitarian benefits. |
| Maccario and Naldi (2023) | Feelings about privacy are divided, with half of the users feeling negative and the other half positive. However, negative perceptions do not affect product feelings, which remain positive. |
| Maroufkhani et al. (2022) | Privacy risk is the most significant barrier influencing the overall perceived value consumers assign to voice assistants. |
| McLean and Osei-Frimpong (2019) | Utilitarian, symbolic, and social benefits motivate users. |
| Mishra et al. (2022) | Utilitarian attitudes have a stronger impact (compared to hedonic attitudes) on both SVA users and SVA use. Those attributing prestige to SVA are more likely to use it as an escape route from everyday life. |
| Molinillo et al. (2023) | Performance expectancy and emotional value influence intentions to continue using the product. |
| Moriuchi (2021) | Anthropomorphism impacts engagement, which then impacts consumer intentions to re-use virtual assistants. |
| Mols et al. (2021) | Increased use correlates with increased concerns about privacy, surveillance, device security, and day-to-day behaviour and transparency. |
| Oliveira et al. (2023) | Customer experience is composed of functional, social, and relational factors, which impact marketing outcomes. This underscores the negative influence of enthusiasm. |
| Pitard and Marriott (2021) | Individuals interact with virtual assistants by treating them as social entities and employing human social norms. |
| Poushneh (2021) | Functional intelligence, sincerity, and creativity allow consumers to take control of their interactions with smart speakers. |

**Appendix 1.1 (Continued).** Voice assistant literature review

| Author/s | Main findings |
|---|---|
| Saavedra et al. (2023) | Virtual assistants‘ perceived usefulness is determined by the quality of the process and the quality of results. This influence is especially significant for innovation-oriented users. |
| Shin et al. (2018) | Compatibility, ease of use, and perceived usefulness have a positive effect on purchase intentions. |
| Song et al. (2022) | Compared with human recovery, chatbot self-recovery enhances consumer service affirmations. Perceived privacy risk is lower in chatbot self-recovery than in human recovery. |
| Vimalkumar et al. (2021) | Trust in the technology and the service provider plays an important role in device adoption practices. |
| Zhou et al. (2023) | Anthropomorphism can enhance a sense of social presence. It can engender companionship, alleviate loneliness, and deliver more comprehensive and valuable information, thereby improving human–computer interactions. |

**Appendix 1.2.** Privacy research

| Author/s | Context | Main findings |
|---|---|---|
| Bandara et al. (2020) | E-commerce | Privacy power is a psychological construct related to individuals‘ perceptions about the degree to which they can control the distribution and use of their personal information. |
| Fox et al. (2021) | Mobile apps | Perceived reciprocal benefits and health benefits associated with mobile apps positively influence willingness to trust. Privacy concerns have a negative, but weak, influence. Individuals‘ future intentions regarding an app are influenced by reciprocal benefits and prior adoption intentions. |
| Kim et al. (2019) | IoT | Users do not pay much attention to privacy risks when provisioning personalised services. |
| Krafft et al. (2017) | Online environment | Permission-granting decisions are primarily based on consumers‘ cost-benefit calculations. Pronounced registration costs, privacy concerns, and anticipated intrusiveness have a negative effect on the likelihood of granting permission. |
| Lee and Rha (2016) | Location-based mobile commerce | There are four distinct consumer groups, identified according to the degree to which they comprehend the personalisation–privacy paradox. These groups are the ambivalent group, the privacy-oriented group, the personalisation-oriented group, and the indifferent group. There are also significant differences in the personalisation–privacy paradox‘s antecedents between the different groups. |
| Li et al. (2017) | Websites | Consumers are more likely to disclose their personal information when they have formed positive emotional and cognitive appraisals of a website. General privacy concerns are found to have a weak effect on online users‘ privacy behaviour. These concerns arise from people‘s individual experiences. |
| Libaque-Sáenz et al. (2021) | Mobile devices | Fair information practices influence consumers‘ assessments of privacy when it comes to adopting a mobile app. They provide consumers with control, and this control influences consumer perceptions and risk-taking behaviour. |
| Martin (2015) | Online environment | Privacy notices are a necessary, but not sufficient, condition for meeting consumers‘ privacy expectations. |
| Taddicken (2013) | Websites | Privacy concerns affect self-disclosure behaviour through factors like social relevance. Social environment and self-disclosure significantly affect user behaviour. Users are willing to let others know things about them but prefer restricted online disclosure (e.g., on social media). |
| Xu et al. (2011) | Websites | A novel model incorporates (a) the characteristics of overt and covert personalisation approaches and (b) personal characteristics in the privacy decision-making process. Personalisation can override privacy concerns in both overt and covert cases. |
| Yu et al. (2020) | Online environment | Perceived privacy risks have significant negative effects on disclosure intentions and behaviour, but privacy concerns can decrease disclosure intentions. Privacy concerns do not significantly affect disclosure behaviour. |
| Abdi et al. (2022) | Smart home personal assistants | Examine privacy standards in the Smart home personal assistants (SPA) ecosystem, taking into account the acceptability of information flows between the various entities involved. These include SPA providers, third-party skill providers, users, and sundry stakeholders. |

**Appendix 1.2 (Continued).** Privacy research

| Author/s | Context | Main findings |
|---|---|---|
| Ammari et al. (2019) | Voice assistants | Most people do not have a coherent view of privacy concerns related to using virtual assistants. Divergences arise when it comes to privacy concerns, and this represents a privacy boundary management problem. |
| Bawack, Wamba and Carillo (2021) | Voice assistants | Trust and privacy concerns mediate the relationship between personality and voice shoppers‘ perceptions during customer experiences. |
| Benlian et al. (2019) | Voice assistants | Involuntary voice activation, high levels of presenteeism, and low user anonymity lead to invasions of privacy. This can, in turn, increase individual stress and household conflicts. Anthropomorphic design features can mitigate and even offset the detrimental effects of privacy invasions on user stress levels. |
| Chung et al. (2017) | Intelligent virtual assistants | Smart speakers have security vulnerabilities that hackers can exploit. |
| Frick et al. (2021) | Smart devices | Trust in smart devices, anxiety, and previous negative experiences are the primary predictors of surveillance perceptions. People with higher computer anxiety also tend to perceive a higher degree of surveillance. |
| Guzman (2020) | Intelligent assistant | People differentiate between humans and computers based on different factors. These include origin, degree of autonomy, intelligence, and emotional capabilities. |
| Lee (2020) | Home IoT | Current and potential users are realistically concerned about the invasion of privacy in a home IoT environment. User vulnerability is an integral antecedent affecting home IoT privacy concerns. |
| Lutz (2020) | Smart home speakers | Privacy is more complex in the smart speaker context than in other environments. This is due to these devices‘ specific technological possibilities. Concerns about third parties listening to smart speaker recordings are especially strong, yet privacy protection behaviours are rare. |
| Malkin et al. (2019) | Smart speakers | Half of smart speaker users are unconcerned about their conversations being recorded. They are, however, more protective of their children‘s or guest‘s recordings. |
| Mani and Chouk (2017) | Smart devices | There is a direct positive relationship between unauthorised secondary use and innovation resistance. The ―big brother effect‖ also has a significant impact on privacy concerns. |
| Manikonda et al. (2018) | Intelligent personal assistant | A significant percentage of home users are concerned about privacy and take action to address their concerns. Privacy concerns increase when people realise that the devices are always listening. |
| McLean and Osei-Frimpong (2019) | Home voice assistants | Privacy risks act as a moderator and weaken the relationship between motives and declared use. |

**Appendix 1.2 (Continued).** Privacy research

| Author/s | Context | Main findings |
|---|---|---|
| Patrizi et al. (2024) | Voice-based AI | Perceived privacy risk positively moderates the relationship between brand anthropomorphism and brand trust. Specifically, brand anthropomorphism‘s influence on brand trust strengthens at high levels of perceived privacy risk. |
| Pitardi and Marriot (2020) | IA agents | Usability and user-friendliness play a significant role in the acceptance and use of advanced intelligent technologies. Emotional reactions play an important role in driving user attitudes toward human-AI interactions. |
| Vimalkumar et al. (2021) | Voice-based digital assistants | Privacy risk has a significant negative influence on perceived trust. The higher the perceived risk, the less trustworthy people perceive the technology to be. The higher the trust in the technology, the higher the technology‘s expected performance. People who see the VBDA as a potential threat to their privacy also show a higher level of concern about the technology. |

# CHAPTER II

## HOW PERSONALISATION CAN IMPROVE ATTITUDE TOWARD INFORMATION COLLECTION BY SMART HOME SPEAKERS

## 2.1. INTRODUCTION

As mentioned in the previous chapter, smart home speakers provide companies with valuable information about their consumers‘ patterns, tastes and preferences that can help them offer good service and excellent experience to their customers, by delivering value to them in a personalised way (Lavado-Nalvaiz et al., 2022). However, while better service is perceived as a benefit by consumers, this collection of information also raises concerns about their privacy (Promfret et al., 2020)

The always-on functionalities of the smart home speakers raises potentially very sensitive issues about how these devices collect and use personal private information (Vimalkumar et al., 2021). Even the daily routines of consumers can be collected, recorded and stored (Chung and Lee, 2018). Despite users‘ privacy concerns the value of personalisation is a sufficient benefit to improve both the willingness of the customer to disclose personal information (Cheng et al., 2021; Kim and Kim, 2018; Vimalkumar et al., 2021) and their willingness to grant permission (Krafft et al., 2017) which involves an overt information collection strategy. However, previous research has suggested that the usefulness of voice assistants is also based on the ability to work with some applications of skills that do not request any permission from the user or even use their personal information without their knowledge (Alepis and Patsakis, 2017; Yang and Lee, 2019). This is known as covert information collection strategy. Then, can the value of personalisation influence user attitudes toward covert data collection and the intention to continue to use the smart home speaker? Despite the relevance of this topic, due to the opportunities that covert information collection gives to companies, few studies have focused on its effects on consumer behaviour (Aguirre et al., 2015; Libaque-Sáenz et al., 2021; Xu et al., 2011), and as far as authors know, no research has examined the antecedents of consumer‘s attitude toward covert information collection.

Based on this gap, this chapter will focus on how perceived personalization of voice assistant recommendations and trust influence the user‘s attitude toward covert and overt information collection.

Under privacy calculus theory, the so-called personalisation–privacy paradox posits that trust in the service provider is another important factor in explaining the disclosure of information (Aguirre et al., 2015; Grosso et al., 2020). In the literature on smart devices, trust explains the user‘s experience of, attitude toward and intention to adopt smart home speakers (Ameen et al., 2021; Bawack, Wamba and Carillo, 2021; Pitardi and Marriott, 2021). However, to the best of our knowledge, no studies have analysed the role of trust in user attitudes toward overt and covert information collection, or in their intention to continue to use the smart home speaker.

This study has three aims. First, it analyses whether the value of receiving personalised information can determine attitude toward the two types of information collection (overt vs. covert). Second, it examines the effect of attitude toward overt and covert information collection on the intention to continue to use the device. Finally, it analyses the role of trust in the relationship between consumer attitude toward covert information collection and intention to continue to use. To achieve these objectives, a survey of 679 users of smart home speakers is conducted, and their responses are analysed using structural equation modelling.

The contribution of this study is threefold. First, it contributes to the growing research around consumers behaviour with voice assistants or AI devices. The research provides new evidence of how the perceived value of personalisation influences attitudes toward how the information is collected. Second, this study contributes by examining the consequences of user attitudes toward covert information collection to

determine the consequences of that strategy from a post-decision perspective. Third, this study provides new evidence of the role of trust in the service provider in influencing that attitude, by examining the mediation-moderation role of trust.

This chapter first sets out the theoretical framework and the underlying theories within which the study is framed. Next, the hypothesised relationships are presented. After this, the methodology and analytical techniques used to obtain the results are explained. Implications for academics and practitioners are discussed. Finally, future lines of research are proposed.

## 2.2. THEORETICAL FRAMEWORK

### 2.2.1. Personalisation

Personalisation is an important marketing strategy for customer relationships. Smart home speakers can offer personalised information when the user makes a query or asks for a recommendation about a product or service, or proactively respond to a customer‘s needs using information collected about preferences, behaviour and needs (Holtrop et al., 2017; Huang, 2018). This type of data is collected during every moment of the business-to-consumer relationship. Therefore, companies face the challenge of accessing the right data on which to base personalisation without negatively affecting customers‘ privacy (Ameen et al., 2021).

Although individuals show a high theoretical interest in the privacy of their information, they often disclose that information in exchange for small rewards, such as saving time in finding the right products, financial gain in terms of access to promotions or special prices, and even friendship or love (Chen et al., 2021; Kang and Jung, 2020; Tan and Liao, 2021; Xu et al., 2011). This contradiction between users‘ stated concern

and their actual behaviour is known as the personalisation–privacy paradox (Dinev and Hart, 2006; Norberg et al., 2007). Under this theory, Dinev and Hart (2006) found a negative relationship between privacy concerns and the willingness to disclose personal information for Internet transactions. The benefits and risks of information disclosure are the antecedents of the value of personalisation that influence willingness to disclose personal information (Dinev and Hart, 2006; Klumpe et al., 2020; Krafft et al., 2017; Xu et al., 2011)

### 2.2.2. Attitude toward information collection

Under the personalisation–privacy paradox, research has mainly examined the situation in which firms request permission (overt information collection). When information is collected overtly, the company notifies consumers of this collection, generating a feeling of trust, transparency and reliability toward the company and control over the information provided (Karyda et al., 2009; Libaque-Sáenz et al., 2021).

Little research has focused on consumer behaviour when information is collected covertly (Aguirre et al., 2015; Hayes et al., 2021; Xu et al., 2011). Aguirre et al., (2015) observed that ‒covert information collection strategies occur when firms collect data without consumers‘ awareness, often by unobtrusively gathering information while the consumer browses the Internet‖ (p. 36). They concluded that this type of information collection benefits consumers, as it does not disrupt their online experience and allows more impartial information to be obtained, making the personalisation experience more complete. Xu et al., (2011) differentiated between these forms of information collection, finding that privacy risks arise when information is collected covertly. In this regard, Libaque-Sáenz et al., (2021) found that covert information collection tends to increase perceived risk regarding the subsequent use of

information, increase the sense of privacy loss associated with data collection, and reduce the perceived control of data.

Consumer attitudes are positive or negative beliefs about a product or some of its functionalities. They are built up from direct experiences with the product and are expected to be strongly related to actual use (Karahanna et al., 1999). Previous research agrees that attitude represents ‗a summary evaluation of a psychological object captured in such attribute dimensions as good–bad, harmful–beneficial, pleasant–unpleasant, and likeable–dislikeable' (Ajzen 2001, p. 29). Therefore, this study focuses on the consumers' attitude toward the smart home speaker's functionality of collecting information overtly and covertly, its antecedents and consequences, contributing to a topic with scarce research (Hayes et al., 2021; Libaque-Sáenz et al., 2021).

### 2.2.3. Trust

Trust has been analysed in different contexts such as e-commerce (Gefen et al., 2003), networking sites (Cheung et al., 2015), trust in information systems (Li et al., 2008) and trust in human–automation interaction (Pitardi and Marriott, 2021; van Pinxteren et al., 2019). In the context of artificial intelligence (AI), recent research shows that trust is a key factor in the acceptance and use of this technology (Fernandes and Oliveira, 2021; Pitardi and Marriott, 2021; Vimalkumar et al., 2021). Analysing the drivers of consumer trust in smart speakers, Pitardi and Marriott (2021) suggested that trust in the service provider is related not only to the intention to use but also to the attitude or predispositions that consumers show in their interactions with voice assistants. Trust in the service provider is defined as the degree to which people believe that a company can be trustworthy in protecting consumers' personal information (Bawack et al., 2021). It implies confidence in the service provider that incorporates elements of honesty, competence and benevolence (Flavián and Guinaliu, 2006).

Previous studies have shown that intangibility and lack of face-to-face interaction increase consumer uncertainty and perceived risk (Ameen et al., 2021; Michler et al. 2020), and that the storage of personal data increases privacy risk (Benlian et al., 2019; Lucia-Palacios and Pérez-López, 2021). Therefore, the current study focuses on the role that trust in the service provider plays in the way information is collected (being competent in data storage, honest about the data collected and benevolent in the use of data) and its relationship with the intention to continue to use.

## 2.3. HYPOTHESES

### 2.3.1. Personalisation, trust and intention to continue to use

In the case of smart home speakers, personalisation makes it possible to provide relevant information and recommendations to consumers based on their interests, activities, locations and routines (Kim et al., 2019). Godey et al. (2016) asserted that personalised services that satisfy individual preferences create greater affinity and ensure loyalty and satisfaction.

Under the personalisation–privacy paradox, tailored messages that fit the consumer‘s preferences and tastes improve the benefit–cost relationship and enhance the attitude toward the message or ad (Campbell and Wright, 2008). When the net benefit of information collection is positive, personalisation reduces perceived information overload, consumers are less concerned about privacy and more likely to disclose their personal information (Jung, 2017). Thus, under the personalisation–privacy paradox, the higher the value and the more relevant the messages, the greater the willingness of consumers to disclose their personal information (Cheng et al., 2021; Kim and Kim, 2018) and the greater their willingness to grant permission (Krafft et al.,

2017). Therefore, if users perceive a high value in receiving personalised recommendations, they will have a more positive attitude toward information collection, whether it is covert or more transparent. Thus, we propose:

**H1:** *The perceived value of personalisation has a positive effect on attitude toward overt information collection.*

**H2:** *The perceived value of personalisation has a positive effect on attitude toward covert information collection.*

If agents‘ recommendations fulfil consumers‘ needs better because they are personalised, users will perceive that the service provider is competent in the use of data collected, being this competence an element of trust (Komiack and Benbasat, 2006). Trust is considered a critical attribute in the beginning, development and maintenance of relationships in different contexts of exchange (Amin, Ahmad and Sang Choi, 2019; Van Pinxteren, 2019). Companies could try to increase consumer confidence through evidence of their benevolence and reliability (Kim and Kim, 2018).

Singh and Sirdeshmukh (2000) have shown that there is a positive and direct relationship between perceived value and trust in service providers. They demonstrated the link between perceived value and trust by showing that trust is a key and central factor during the exchange. Similarly, in the online services context, several studies support the claim that perceived value and trust in the service provider are strongly related (Ameen et al., 2021; Bawack et al., 2021). Accordingly, this study proposes that a higher perceived value of smart home speaker personalisation will generate more trust in smart home speaker providers and their use. Therefore, we propose:

**H3**: *The perceived value of personalisation has a positive effect on trust.*

Previous research supports the idea that a higher value of personalisation is a greater benefit, and that this will lead users to have a higher intention to use the device (Volchek et al., 2021). Ashfaq et al. (2021) demonstrated that a high perceived value of smart home speakers improves user attitudes to the devices and increases their intention to continue using them. Likewise, in a study on creating value for tourists through personalised messages, Volchek et al. (2021) concluded that showing personalised advertisements and offering tailored recommendations to users who visit tourism websites improved value and, in turn, usefulness and their intention to use these websites. Thus:

**H4:** *The perceived value of personalisation has a positive effect on intention to continue to use.*

Generally, consumer trust in a company is an important predictor of consumer actions regarding the firm and the services it offers (Gefen et al., 2003). Trust in a service provider will play an important role in the development of consumer behaviour, including purchase intentions, usage intentions and adoption of voice-based digital assistants (Ameen et al., 2021; Fernandes and Oliveira, 2021; Pitardi and Marriott, 2021; Vimalkumar et al., 2021). Consumers‘ trust in service providers can help to reduce their cognitive risk and insecurity, thereby promoting not only purchase intention but also the development of a long-term relationship (Laaksonen et al., 2009). Furthermore, a high level of trust in service providers will lead to continued purchase and use, while a lack of trust will lead to exactly the opposite (Yang et al., 2015). Given the limited consumer understanding of how data is collected, stored, analysed and used by voice assistants to offer personalised services (often referred to as black box), all the interactions with voice assistants require trust in the use of these devices. Thus, we propose:

**H5:** *Trust has a positive effect on intention to continue to use.*

Trust in the company or service provider plays a key role in making consumers feel more secure in sharing their personal information (Schaupp and Carter, 2010). Bleier and Eisenbeiss (2015) argued that trust in a firm can make consumers believe that their personal data is in good hands, thus alleviating potential privacy concerns. Bansal et al. (2016) argued that trust is positively associated with the intention to disclose information in the context of finance and e-commerce. Trust can reduce the perception of privacy risks (Zimmer et al., 2010), so users with a high level of trust are more comfortable with the interaction with the device and willing to disclose personal information (Mesch, 2012). This self-disclosure can happen even without requesting overtly that information during the interaction as consumers trust the service provider. Since they believe that the service provider is benevolent, they are also more likely to believe that it will protect and keep their personal data safe (Bleier and Eisenbeiss, 2015). They will be less worried about the non-transparent ways in which cover data collection is processed and may even believe that is a good option since it can save them time and make better decisions (Payne et al., 2021). Therefore, they may show a more favourable attitude toward covert information collection as well. So, we propose:

**H6:** *Trust has a positive effect on attitude toward overt information collection.*

**H7:** *Trust has a positive effect on attitude toward covert information collection.*

The relationship between attitude and intention has been widely examined under the technology adoption model (Davis et al., 1989). Previous research has found that attitude is a powerful predictor of intention to continue to use a technology (Amoroso and Lim, 2017; Wu and Chen, 2017). Regarding smart products, some studies have found a significant positive effect of attitude toward the device on the intention to

continue to use (Pitardi and Marriott, 2021). No previous research has examined the relationship between user attitudes toward how information is collected and their intention to continue using the smart product. Nevertheless, following previous research on the adoption of innovations, we propose that a positive attitude toward how private information is collected (overtly vs. covertly) will lead to a higher intention to continue using the smart home speaker. Thus, we propose:

**H8:** *Attitude toward overt information collection has a positive effect on intention to continue to use*.

**H9:** *Attitude toward covert information collection has a positive effect on intention to continue to use*.

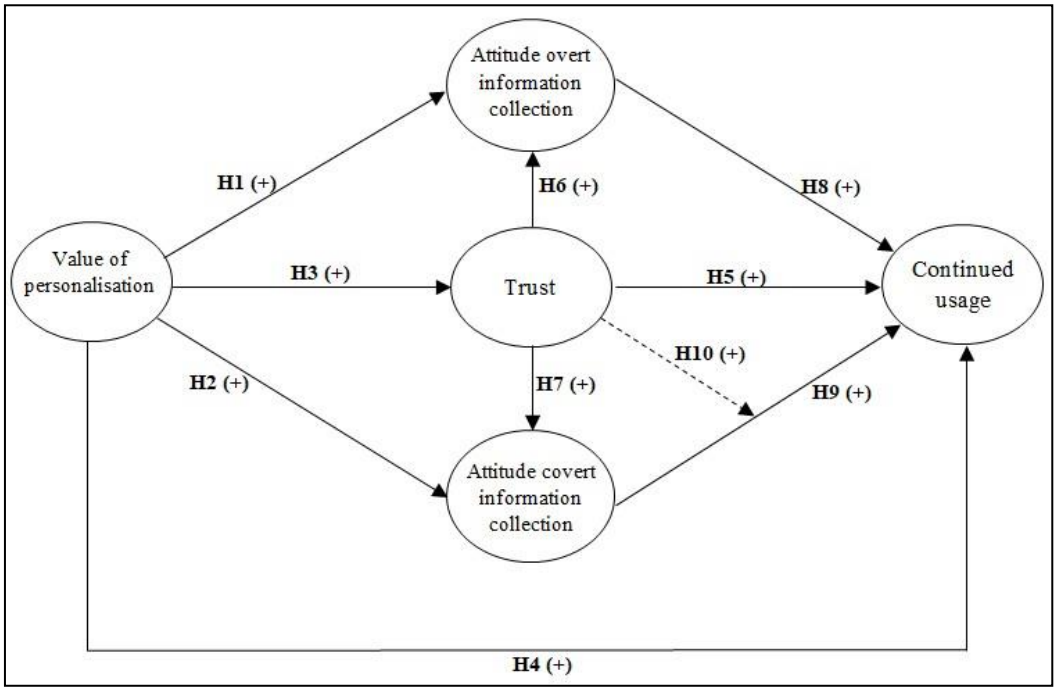
### 2.3.2. Moderating effect of trust

Users are sometimes unable to know how or why companies are collecting and using the information they provide about their purchases (Lau et al., 2018). They also do not know whether the company is acting from self-interest or to generate greater added value in the purchasing process (Yuan et al., 2019). Pavlou et al. (2007) asserted that users are more likely to accept a sense of vulnerability about trustworthy websites. Within the context of online advertising, Aguirre et al. (2015) found that a more trustworthy website can mitigate the negative effects of covert data collection when clicking on advertising messages. Users who are not comfortable with a firm‘s privacy policy strategy are less willing to return to its website. Alashoor et al. (2017) indicated that high levels of trust in a website could weaken the negative relationship between privacy concerns and self-disclosure. In the retail context, Grosso et al. (2020) found that trust in a retail company moderates the negative relationship between privacy concerns and willingness to disclose information, such that high levels of retailer trust

mitigate this negative relationship. In this case of study, this thesis did not test privacy concerns, but the attitude toward covert information collection. Based on this, and previous research, it is proposed that for those users with greater trust in the service provider, a positive attitude toward covert information collection will have a stronger positive effect on continued usage than for users whose trust is lower. Similarly, those who do not have a positive attitude toward information collection should show a lower intention to continue to use the device. That negative effect could be diluted if users trust the firm, as they think the information collected will be used to provide a better and more personalized service and that their personal data will be safe (Pavlou et al., 2007; Yuan at al., 2019). So, we propose:

**H10:** *Trust will have a positive moderating effect on the relationship between attitude toward covert information collection and intention to continue to use.*

**Figure 2.1.** Theoretical model



## 2.4. METHODOLOGY

The research hypotheses were tested against data collected using a survey questionnaire administered on Mechanical Turk (MTurk) in May 2021. All participants are American, over 18 years of age, own a smart home speaker and English is their primary language, so the survey was developed and distributed in English. Initially, 700 responses were obtained. Some questionnaires were eliminated because the answers of the respondents followed a pattern or they answered one of the control questions incorrectly. This yielded a total of 679 valid responses.

Measurement of the variables was carried out in line with previous research. All constructs are reflective and measured using a seven-point Likert scale, from 1 = completely disagree to 7 = completely agree.

The dependent variable, intention to continue to use, is a construct formed from three items based on previous research (Bhattacherjee 2001; Han and Yang 2018). The perceived value of personalisation was measured using three items proposed by Xu et al. (2011). The attitude construct was adopted from Lee et al. (2012), which consists of four items that we adapted according to the definition of the covert strategy proposed by Aguirre et al. (2015; see Section 2.2 above). Previous to that, a definition of covert information was provided in the survey. The trust construct was adapted from Lee and Rha (2016). These variables and their items can be found in Appendix 2.1.

Control variables were also included: education, a categorical variable comprising four levels; gender, a dummy variable; age was an open-ended response and frequency of use was also a categorical variable comprising five levels.

### 2.4.1. Descriptive results

Table 2.1 describes the sample in terms of gender, education, brand, income, frequency of use and age. The results show that there is variability in the control variables and that respondents did not conform to any specific user profile. Of the respondents, 55.52% were female, and 61.86% had a higher education level (i.e., were graduates). The respondents were clustered in the middle-income levels, with 46.84% of them earning between $40,000 and $79,999. As expected, given the product under study, 56.35% of respondents were between 24 and 35 years old. In addition, 50.66% reported using their smart home speaker almost every day. Of the brands specified in the survey, the most common was Alexa (Amazon), owned by 65.87% of respondents, followed by Google Home (Google), owned by 23.27%.

**Table 2.1.** Sample characteristics

| Gender (%) | | Education (%) | | Frequency (%) | | Brand (%) | | Income $ (%) | | Age (%) | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| F | 55.52 | N | 1.03 | N | 0.44 | Alexa | 65.87 | < 20,000 | 5.30 | 18–24 | 3.09 |
| M | 44.48 | C | 7.36 | AN | 1.62 | Cortana | 1.07 | 20,000–39,999 | 11.93 | 25–34 | 56.55 |
| | | B | 61.86 | S | 17.38 | Google Home Pod | 23.27 | 40,000–59,999 | 24.45 | 35–44 | 23.71 |
| | | M/PhD | 29.75 | AED | 50.66 | | 9.79 | 60,000–79,999 | 22.39 | 45–54 | 10.75 |
| | | | | ED | 29.99 | | | 80,000–99,999 | 23.56 | 55–64 | 4.27 |
| | | | | | | | | > 100,000 | 12.08 | > 65 | 1.62 |
| | | | | | | | | No disclosure | 0.29 | | |

***Note*** *F, Female; M, Male; N, None; C, College; B, Bachelor; M/PHD, Master/PhD; N, Never; AN, Almost never; S, Sometimes; AED, Almost every day; ED, Every day.*

## 2.5. RESULTS

### 2.5.1. Common method bias

Common method variance could pose a serious problem. In order to control it, a procedural control and statistical control was established. Regarding the procedure, in order to ensure that the dependent and independent variables were psychologically

separated, the questions and survey items were randomly ordered. In this way, the researchers' interest was concealed and the relationship between dependent and independent variables was hidden (Podsakoff et al., 2012). Additionally, according to MacKenzie and Podsakoff (2012), respondents were told that all responses were anonymous and that there were no correct answers.

Regarding statistical control, Harmon‘s one-factor test was conducted for the whole sample. The results showed that a single factor explained 22.12% of the variance; when all the factors in the model were taken into account, the variance explained increased to 74.15%. Thus, there is no indication of any problem with common method variance. In addition, the model was run using a new "random" variable (a single indicator latent variable) to obtain the variance inflation factor (VIF) values of all variables in the model (Kock and Lynn, 2012). The results show that the VIF values are equal to or less than 3.3, so the model can be considered free of common method bias (see table 2.2).

### 2.5.2. Measurement model validation

An exploratory factor analysis was carried out using SPSS software to check the dimensionality of the reflective constructs. Confirmatory factor analysis was conducted using SmartPLS 3.3 software and revealed a solution of five constructs. None of the indicators were eliminated, as they did not have factor loadings of less than 0.5 (Carmines and Zeller, 1979) (see Table 2.2).

**Table 2.2.** Items and measurement model

| | VIF | Loadings | Cronbach's alpha | Composite reliability | AVE | Mean | Standard deviation |
|---|---|---|---|---|---|---|---|
| **Value of personalisation** | 1.36 | | 0.803 | 0.884 | 0.717 | 5.253 | 1.011 |
| VALUE_1 | | 0.861 | | | | | |
| VALUE_2 | | 0.835 | | | | | |
| VALUE_3R | | 0.844 | | | | | |
| **Continued usage** | 2.11 | | 0.749 | 0.857 | 0.667 | 5.371 | 0.832 |
| CONT_1 | | 0.862 | | | | | |
| CONT_2 | | 0.753 | | | | | |
| CONT_3 | | 0.830 | | | | | |
| **Trust** | 1.89 | | 0.911 | 0.938 | 0.790 | 4.961 | 1.151 |
| TRUST_1 | | 0.894 | | | | | |
| TRUST_2 | | 0.882 | | | | | |
| TRUST_3 | | 0.888 | | | | | |
| TRUST_4 | | 0.892 | | | | | |
| **Att information collection (overt)** | 2.06 | | 0.793 | 0.865 | 0.617 | 5.223 | 0.879 |
| OVERT_1 | | 0.787 | | | | | |
| OVERT_2 | | 0.796 | | | | | |
| OVERT_3 | | 0.745 | | | | | |
| OVERT_4 | | 0.810 | | | | | |
| **Att information collection (covert)** | 2.15 | | 0.946 | 0.961 | 0.861 | 4.395 | 1.603 |
| COVERT_1 | | 0.939 | | | | | |
| COVERT_2 | | 0.923 | | | | | |
| COVERT_3 | | 0.919 | | | | | |
| COVERT_4 | | 0.931 | | | | | |

For all constructs, Cronbach's alpha values and the composite reliability index exceeded the recommended minimum of 0.7 (Bagozzi and Yi, 1988; Nunnally, 1978), confirming internal consistency. Concerning convergent validity, the values of the AVE were above 0.5 for all the latent variables (Fornell and Larcker, 1981).

Discriminant validity was evaluated using Fornell and Larcker's (1981) criterion and the heterotrait–monotrait (HTMT) ratio (Henseler, Ringle and Sarstedt, 2015). The squared roots of AVE were higher than the correlations between pairs of constructs (Table 2.3), and the HTMT ratios were below the threshold of 0.85 for all the latent variables. Thus, both criteria confirm discriminant validity.

**Table 2.3.** Discriminant validity

| | CONT | COVERT | OVERT | TRUST | VALUE |
|---|---|---|---|---|---|
| **CONT** | **0.817** | 0.164 | 0.411 | 0.566 | 0.487 |
| **COVERT** | 0.139 | **0.928** | 0.283 | 0.453 | 0.600 |
| **OVERT** | 0.319 | 0.255 | **0.785** | 0.382 | 0.534 |
| **TRUST** | 0.469 | 0.421 | 0.332 | **0.889** | 0.654 |
| **VALUE** | 0.381 | 0.523 | 0.430 | 0.561 | **0.847** |

***Note**: Values on the diagonal are square roots of the AVE. Values below the diagonal are correlations between variables. Values above the diagonal are values of the HTMT ratio. COVERT, Attitude covert information collection; OVERT, Attitude overt information collection; CONT, Intention to continue to use; TRUST, trust; VALUE, Perceived value of personalisation.*

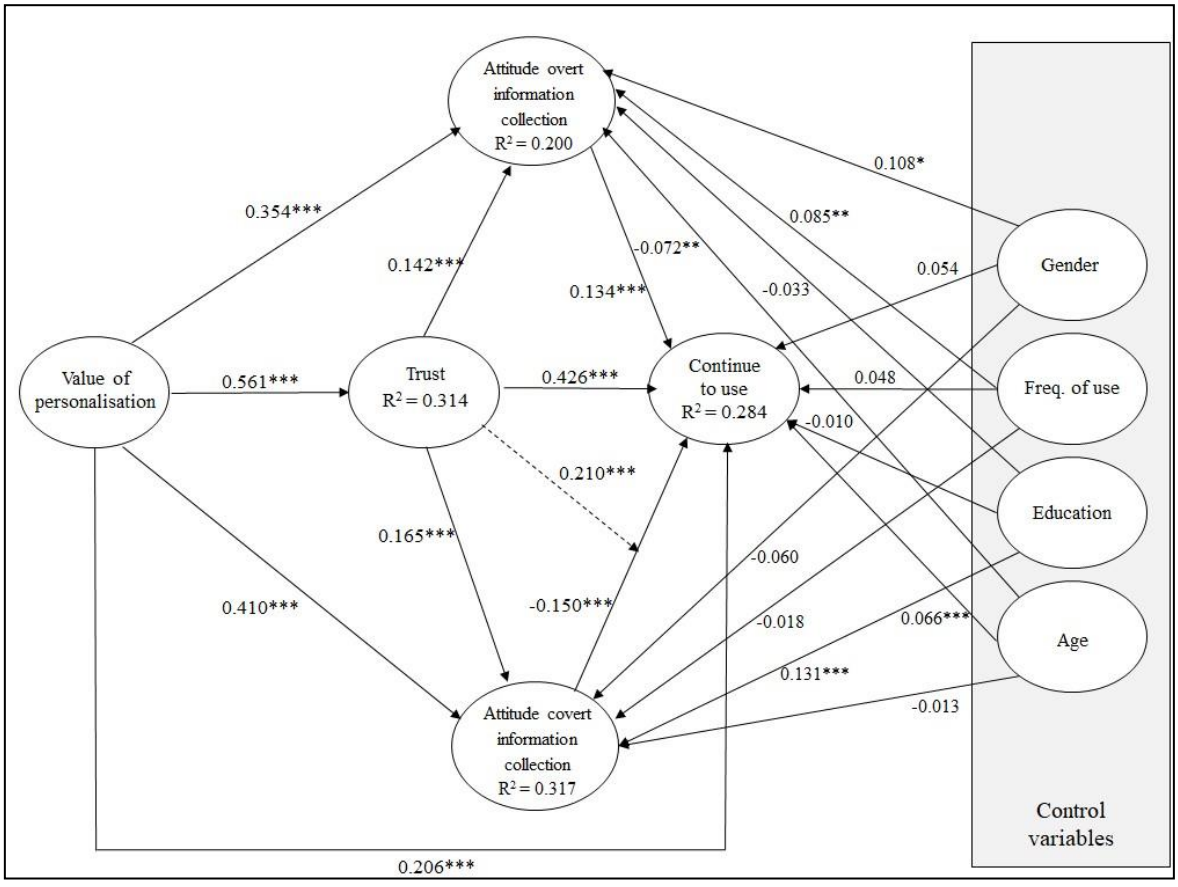
### 2.5.3. Hypothesis testing

The model was estimated by applying SEM using SmartPLS 3.3 software and a bootstrapping of 5,000 subsamples. To test predictive relevance, this software provides the $Q^2$ proposed by Stone and Geisser. According to the results, the $Q^2$ measures were adequate (attitude toward covert information collection = 0.268; attitude toward overt information collection = 0.119; continued usage = 0.182; and trust = 0.246).

The results (Figure 2.2) suggest that the perceived value of personalisation has a direct, positive and significant effect on attitude toward information collection, both overt and covert, which supports H1 and H2. The results also show a positive and significant relationship between the perceived value of personalisation and trust, which supports H3. As there is a positive and significant relationship between perceived value and continued usage, H4 is supported. Trust has a positive and significant effect on the intention to continue to use, as well as on attitude toward information collection, both overt and covert, supporting H5, H6 and H7. In addition, H8 is supported, as the results show a direct, positive and significant relationship between attitude toward the collection of information in an overt way and intention to continue to use. However, H9 is not supported, as the results show a negative relationship between attitude toward the collection of information in a covert way and intention to continue to use the device.

Regarding the control variables, education positively and significantly affects user attitudes toward covert information collection. Therefore, people with a higher level of education are more likely to have a positive attitude toward covert information collection. Additionally, age affects positively and significantly intention to continue to use and negatively and significantly user attitudes toward overt information collection. Thus, older people are more likely to continue to use the smart home speaker while younger people tend to have a positive attitude toward overt information collection. Frequency of use and gender positively and significantly affects user attitudes toward overt information collection. Therefore, men and frequent device users are more likely to have a positive attitude toward overt information collection.

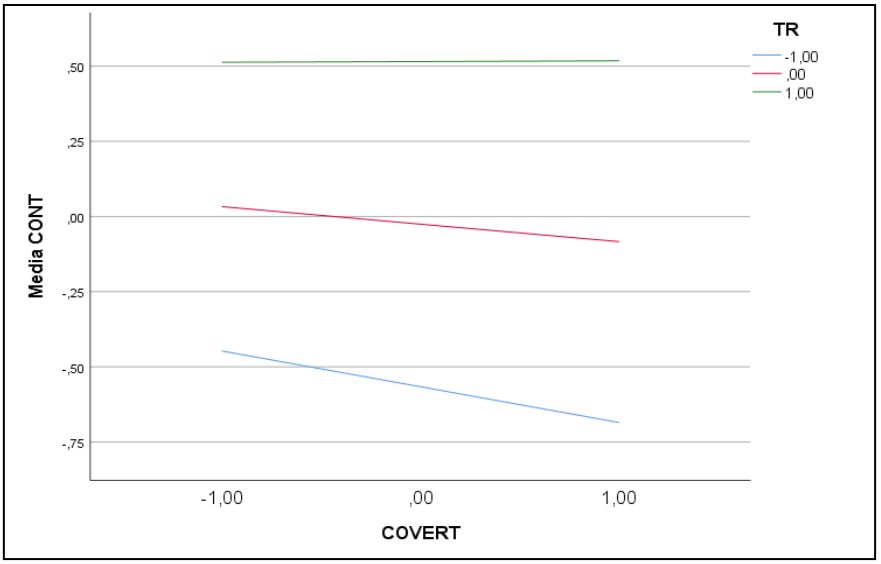
**Figure 2.2.** Results of the structural model




***Note**: *p<0.1; **p<0.05; ***p<0.01*

In terms of the moderating effect of trust, this chapter proposed that trust would positively moderate the relationship between attitude toward covert information collection and intention to continue to use. However, the results show that this main relationship is negative and consequently, the theoretical argumentation of H10 cannot be supported, as the moderation had been proposed on a positive and not on a negative relationship. Figure 2.3 shows the moderating effect of trust on the relationship between attitude toward covert information collection and intention to continue to use the smart home speaker. When trust is high, the relationship between the attitude to the covert collection of information and the intention to continue to use becomes less negative. For trusted users, this relationship  stable, with no changes in the slope. For trusted users, the impact of attitude toward covert information collection on continue to use is stable for any value of users' attitude.

**Figure 2.3.** Moderating effect of trust on the relationship between attitude toward covert information collection and intention to continue to use




***Note*** *COVERT, Attitude covert information collection; CONT, Intention to continue to use; TR, trust.*

We checked the mediating effect of trust in this model. The results (Table 2.4) show that the main mediating effect of trust is found in the path Value-Trust-Continue

to use. Trust exerts a partial mediating effect in this case. The other mediating effects are small.

**Table 2.4.** Indirect effects

| | Effect | BootSE | BootLLCI | BootULCI |
|---|---|---|---|---|
| VALUE → TRUST →CONT | 0.235 | 0.030 | 0.195 | 0.315 |
| VALUE →TRUST →COVERT →CONT | -0.012 | 0.006 | -0.024 | -0.003 |
| VALUE →TRUST →OVERT →CONT | 0.010 | 0.059 | 0.002 | 0.024 |

***Note**: COVERT, Attitude covert information collection; OVERT, Attitude overt information collection; CONT, Intention to continue to use; TRUST, trust; VALUE, Perceived value of personalisation.*

Additionally, we found it instructive to conduct a moderated mediation analysis. Hayes' Syntax approach was employed to check whether the indirect effect of perceived value on intention to continue to use, mediated by trust and attitude toward covert information collection is moderated by trust. The index of moderated mediation is 0.0294, bootstrap 95% CI = (0.0083, 0.0539). Therefore, the indirect effect of the value of personalization on intention to continue to use, mediated by trust and attitude toward covert information collection is less negative for higher levels of trust. Table 2.5 summarises the results of the structural model, which supports all the proposed hypotheses except H9 and H10.

**Table 2.5.** Results of hypothesis testing

| Relationship | Effect proposed | Results | Without moderating effect | | | With moderating effect | | |
|---|---|---|---|---|---|---|---|---|
| | | | p.e | t-statistic | p-value | p.e | t-statistic | p-value |
| **H1** VALUE →OVERT | Positive | Supported | 0.354 | 7.438 | 0.000 | 0.354 | 7.781 | 0.000 |
| **H2** VALUE →COVERT | Positive | Supported | 0.410 | 8.532 | 0.000 | 0.41 | 8.549 | 0.000 |
| **H3** VALUE →TRUST | Positive | Supported | 0.561 | 15.347 | 0.000 | 0.561 | 16.17 | 0.000 |
| **H4** VALUE →CONT | Positive | Supported | 0.18 | 3.535 | 0.000 | 0.206 | 3.779 | 0.000 |
| **H5** TRUST →CONT | Positive | Supported | 0.388 | 9.259 | 0.000 | 0.426 | 9.165 | 0.000 |
| **H6** TRUST →OVERT | Positive | Supported | 0.142 | 3.017 | 0.003 | 0.142 | 3.123 | 0.002 |
| **H7** TRUST →COVERT | Positive | Supported | 0.165 | 3.536 | 0.001 | 0.165 | 3.296 | 0.001 |
| **H8** OVERT →CONT | Positive | Supported | 0.151 | 3.278 | 0.001 | 0.134 | 2.647 | 0.008 |
| **H9** COVERT →CONT | Positive | Not supported | -0.152 | 3.314 | 0.001 | -0.150 | 3.150 | 0.002 |
| **H10** COVERT * TRUST → CONT | Positive | Not supported | - | - | - | 0.071 | 2.82 | 0.005 |

## 2.6. DISCUSSION

This study analyses whether the value of receiving personalised information impacts attitudes toward the two types of information collection (overt vs. covert). Furthermore, it examines the effect of attitude toward overt and covert information collection on intention to continue to use the device and analyses the role of trust in the relationship between consumer attitude toward covert information collection and intention to continue to use.

The results show that the perceived value of message personalisation is positively related to the attitude of users toward both overt and covert information collection, in line with previous studies that have examined the relationship between personalisation and willingness to disclose personal information (Cheng et al., 2021; Libaque et al., 2021). This means that when messages provide greater value and are more relevant, users will have a better attitude toward personal information collection, even if it is collected covertly. As hypothesised, the perceived value of message personalisation has a positive influence on the continued use of the device, confirming the findings of previous studies (Ashfaq et al., 2021; Kim et al., 2017; Volchek et al., 2021). This indicates that consumers will continue to use the device if it offers value through personalisation and delivers relevant messages.

Additionally, the results confirm that the attitude of users toward information collection is positively related to the intention to continue to use the smart home speaker when the information collection is carried out overtly. Again, this is in line with previous research (Libaque-Sáenz et al., 2021; Wu and Chen, 2017). However, against our expectations and in disagreement with previous studies, the results show that the influence of attitude toward covert information collection on the intention to continue

using the device is negative. We have defined attitude toward covert information collection as the consumer‘s positive beliefs about this type of information collection. We considered this definition as the most appropriate based on previous research on the concept of attitude and following the psychology literature that states that positive attitudes lead to action (i.e., continue using the smart home speaker), while negative attitudes lead to inaction (e.g., stop using the device) (Hepler and Albarracin, 2014). While it is true that a negative correlation between favourable attitudes toward covert information collection and intention to continue using the smart home speaker does not seem to make much sense, it must be taken into account that some previous research has already questioned the ‒sacred‖ attitude-intention link (Carrus et al. 2021; Fraj et al., 2022). Bagozzi (1992) stated that while ‒*attitude can activate intentions, certain social psychological conditions may also be present or forthcoming accompanying instigators of intentions*‖ (p. 184). For example, convenience, moral norms, emotions and consciousness may intervene in this link (Coskun and Özbük, 2020). So, it is possible that even consumers showing a not favourable attitude toward covert information collection, may continue using the smart home speaker because of convenience aspects. Furthermore, some additional variables could explain this result such as privacy concerns or information sensitivity. Nevertheless, more research is needed to clarify the negative effect of attitude toward covert information collection on the intention to continue using the smart home speaker.

The findings show the important role of trust in information management. First, the positive effects between value and trust as well as between trust and intention to continue to use have been confirmed, in line with previous research (Ameen et al., 2021; Fernandes and Oliveira, 2021; Pitardi and Marriott, 2021; van Pinxteren et al., 2019; Vimalkumar et al., 2021). Trust plays an important role as we find that a greater

feeling of trust in the smart home speaker vendor leads to a higher intention to continue to use the product. According to previous studies (Liao et al., 2019; Wang et al., 2019), this makes sense, because if the consumer accepts the vendor‘s word and the vendor does not take advantage of their vulnerability, a feeling of security and trust will be generated that will guarantee greater use of the device. Furthermore, this study confirms that trust plays a mediating role between perceived value and intention to continue to use. Guo et al. (2016), for example, used trust in their model as a total mediating factor in adoption intention. Results agree with their finding that trust plays a mediating role between value of personalisation and use.

Regarding the moderating effect of trust, results show that trust moderates the negative relationship between attitude toward covert information collection and continue to use. The fact that the main moderating relationship is negative rather than positive prevents us from drawing appropriate conclusions. It could be suggested that if the user has a positive attitude toward the fact that the device collects information covertly and has a lot of trust in the company, the negative direct effect of the attitude toward covert information on continued use is attenuated. This leaves the door open for future research to examine whether trust can help diminish the negative effect that attitudes toward covert information collection have on the intention to continue using the product. Additionally, the moderated mediation effect is examined. This result shows that trust moderates the indirect effect of the value of personalisation on continue to use mediated by trust and attitude toward information collection.

Concerning the control variables, people with higher levels of education are more likely to have a positive attitude toward covert information collection. In this connection, previous research has found that people with higher levels of education also tend to be more aware of the information that is collected and stored to carry out the

personalisation of services and advertising. This higher level of awareness is positively related to lower levels of concern with privacy (Smit et al. 2014). Regarding gender differences, our results show that men are more likely than women to have a positive attitude toward overt information collection. Previous research has found that women are more concerned than men about their privacy in the online environment (Tifferet 2019) and are more likely to apply protective behaviour (Lin and Wang 2019). Thus, more research is needed to better understand these differences in behaviour between men and women about privacy and intrusiveness. Regarding age, our results show that older individuals are more willing to continue using the product than younger people. Previous studies have noted that older people tend to be more loyal than younger people when it comes to product usage and adoption (Heerink et al., 2010). In contrast, our results show that younger people are more likely to have a positive attitude toward overt information collection.

## 2.7. CONCLUSIONS

### 2.7.1. Research contribution

This study makes several contributions to the literature on information management research and smart technologies. First, this study contributes to privacy calculus theory and information management research by focusing on how information is collected (overtly or covertly). Research on the personalisation–privacy paradox has focused on consumer behaviour when firms request personal information (Dinev and Hart, 2006; Klumpe et al., 2020; Wang et al., 2019), and little attention has been paid to consumer responses to personalised messages when firms collect personal information without requesting permission. Furthermore, although attitude is a variable that is often

analysed in innovation adoption models, it has yet to be examined in the context of the personalisation–privacy paradox, where willingness to disclose is the main consumer behaviour under study. Therefore, this research offers clarification of how the main benefit of disclosing personal information can act as an antecedent of attitude toward the both overt and covert collection of personal information.

Second, previous research has established that privacy and intrusiveness are two main barriers for adoption and use of smart devices that listen to the environment all the time (Benlian et al. 2019). The findings contribute to privacy reseach by providing new strategies that can help to change consumers‘ privacy concerns. Messages that are valuable and personalised can demonstrate to consumers the use that the device is making of the information collected, thereby reducing their concerns, improving their attitude toward covert information collection, and making them more likely to accept that firm‘s strategy. To make this contribution, this research adopts a post-purchase perspective, in contrast to the pre-purchase perspective that is characteristic of personalisation–privacy paradox and adoption research.

This study also contributes to privacy research and to research on smart devices by examining an aspect that has rarely been analysed. Previous research has focused on the adoption of smart devices, including the use or adoption of smart speakers, (Ashfaq et al., 2021; McLean and Frimpong, 2019), trust (Pitardi and Marriott, 2021), intrusiveness (Benlian et al., 2019) and interactivity (Lucia-Palacios and Pérez-López, 2021). However, to date, no research has examined in detail the impact of the use of covert and overt information collection strategies on consumer behaviour. Lucia-Palacios and Pérez-López (2021) considered how interactivity can reduce perceived intrusiveness, and Benlian et al. (2019) focused on the use of anthropomorphism to reduce that perception. However, neither study examined directly the cause of the

intrusiveness, namely covert information collection. Thus, the present study contributes to a new line of privacy research about smart devices and the ethical implications of the covert information-gathering strategy known as passive listening.

Third, the findings contribute to research on the personalisation–privacy paradox and smart products by clarifying the role of trust. Although trust has been included in personalisation–privacy paradox research as a moderating factor to reduce privacy concerns about disclosing personal information, in smart products research it has mainly featured as an antecedent of attitude, and adoption (Gupta et al., 2021) or intrusiveness (Lucia-Palacios and Pérez-López, 2021), or as a main dependent variable (Foehr and Gergelmann, 2020). In contrast, this study offers new evidence for the mediating role of trust between perceived value and intention to continue to use. The findings also indicate that trust has a moderating effect on the indirect effect of the value of personalisation to continue to use through trust and attitude toward covert information collection. Therefore, trust is established as a relevant aspect to improve users' attitudes toward the two information collection strategies, as well as to encourage users to continue using the device.

### 2.7.2. Managerial implications

From a practical point of view, this study has implications for the technology and smart device development sector. First, smart home speaker vendors should offer users a personalised device experience, as the value of receiving personalised information generates greater continuity of use and, even more importantly, improves users' attitudes, regardless of how their private information is collected.

The main managerial implication of this study concerns the effect of how the information collected can influence on the continued use of the product. The users will

continue to use the product if they have a positive attitude toward the overt and transparent collection of personal information. In contrast, a positive attitude toward covert information collection leads to reduced intentions to continue to use the device. Managers should take into account that this negative effect is absent for trusting users. Thus, it is important that managers can create trust in the service provider, so attitude toward covert information collection is not relevant in determining users' intentions to continue using the smart home speaker. Therefore, managers, designers and vendors of these devices must reassure users that their personal data is being collected openly, providing them with information about how, when and what information is being collected in order to increase trust. In this regard, this study demonstrates the importance of trust in the service provider for users. Greater trust improves the attitude of these users and increases their intention to continue using the product. Thus, providers of these devices and services need to develop strong and secure transparency, as well as privacy and security policies that reassure users that the company is making proper use of their personal data, regardless of how it is collected.

### 2.7.3. Research limitations and future research suggestions

Although this study has considerable theoretical and practical implications for providers of this technology, several limitations provide opportunities for future research. One of the limitations lies in the fact that the moderating hypothesis has been proposed based on the moderation of a positive relationship and not a negative one as was ultimately the case in the study. Therefore, future research could analyse whether trust can help to diminish the negative effect that users' attitudes toward covert information collection have on the intention to continue using the product. In addition, it would be useful to conduct further studies to establish whether there are differences for a range of variables, including country, device brand, user age and experience. Another

limitation is the omission of potential moderating variables, such as frequency of use and privacy security. Future studies should seek to take account of these variables, as they could help to explain the negative effect of attitude toward covert information collection on intention to continue to use. Moreover, it would be of value to examine other aspects that can explain consumer intention to continue to use smart home speakers and their attitude toward overt and covert information collection. For example, consumers may already have some expectations, before any use, about how these devices collect information, and so it is worth determining how the confirmation or disconfirmation of these expectations can affect their intention to continue to use the product.

## REFERENCES


Aguirre, E., Roggeveen, A. L., Grewal, D., & Wetzels, M. (2016). The personalization-privacy paradox: Implications for new media. *Journal of Consumer Marketing*, *33*(2), 98-110.

Ajzen, I. (2001). Nature and operation of attitudes. *Annual Review of Psychology*, *52*(1), 27-58.

Alashoor, T., Han, S., & Joseph, R. C. (2017). Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: An APCO model. *Communications of the Association for Information Systems*, *41*(1), 4.

Alepis, E., & Patsakis, C. (2017). Monkey says, monkey does: security and privacy on voice assistants. *IEEE Access*, *5*, 17841-17851.

Ameen, N., Tarhini, A., Reppel, A., & Anand, A. (2021). Customer experiences in the age of artificial intelligence. *Computers in Human Behavior*, *114*, 106548.

Amin, F., Ahmad, A., & Sang Choi, G. (2019). Towards trust and friendliness approaches in the social Internet of Things. *Applied Sciences*, *9*(1), 166.

Amoroso, D., & Lim, R. (2017). The mediating effects of habit on continuance intention. *International Journal of Information Management*, *37*(6), 693-702.

Ashfaq, M., Yun, J., & Yu, S. (2021). My smart speaker is cool! perceived coolness, perceived values, and users‘ attitude toward smart speakers. *International Journal of Human–Computer Interaction*, *37*(6), 560-573.

Bagozzi, R. P. (1992). The self-regulation of attitudes, intentions, and behavior. *Social Psychology Quarterly*, 178-204.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, *16*, 74-94.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management*, *53*(1), 1-21.

Bawack, R. E., Wamba, S. F., & Carillo, K. D. A. (2021). Exploring the role of personality, trust, and privacy in customer experience performance during voice shopping: Evidence from SEM and fuzzy set qualitative comparative analysis. *International Journal of Information Management*, *58*, 102309.

Benlian, A., Klumpe, J., & Hinz, O. (2020). Mitigating the intrusive effects of smart home assistants by using anthropomorphic design features: A multimethod investigation. *Information Systems Journal*, *30*(6), 1010-1042.

Bhattacherjee, A. (2001). Understanding information systems continuance: An expectation-confirmation model. *MIS quarterly*, 351-370.

Bleier, A., & Eisenbeiss, M. (2015). The importance of trust for personalized online advertising. *Journal of Retailing*, *91*(3), 390-409.

Campbell, D. E., & Wright, R. T. (2008). Shut-up i don't care: understanding the role of relevance and interactivity on customer attitudes toward repetitive online advertising. *Journal of Electronic Commerce Research*, *9*(1).

Carmines, E. G., & Zeller, R. A. (1979). *Reliability and validity assessment*. Sage publications.

Carrus, G., Tiberio, L., Mastandrea, S., Chokrai, P., Fritsche, I., Klöckner, C. A., ... & Panno, A. (2021). Psychological predictors of energy saving behavior: a meta-analytic approach. *Frontiers in Psychology*, *12*, 648221.

Cheng, X., Hou, T., & Mou, J. (2021). Investigating perceived risks and benefits of information privacy disclosure in IT-enabled ride-sharing. *Information & Management*, *58*(6), 103450.

Cheung, C., Lee, Z. W., & Chan, T. K. (2015). Self-disclosure in social networking sites: the role of perceived cost, perceived benefits and social influence. *Internet Research*, *25*(2), 279-299.

Chung, H., & Lee, S. (2018). Intelligent virtual assistant knows your life. *arXiv preprint arXiv:1803.00466*.

Coşkun, A., & Özbük, R. M. Y. (2020). What influences consumer food waste behavior in restaurants? An application of the extended theory of planned behavior. *Waste Management*, *117*, 170-178.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982-1003.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61-80.

Fernandes, T., & Oliveira, E. (2021). Understanding consumers‘ acceptance of automated technologies in service encounters: Drivers of digital voice assistants adoption. *Journal of Business Research*, *122*, 180-191.

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. *Industrial Management & Data Systems*, *106*(5), 601-620.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39-50.

Foehr, J., & Germelmann, C. C. (2020). Alexa, can I trust you? Exploring consumer paths to trust in smart voice-interaction technologies. *Journal of the Association for Consumer Research*, *5*(2), 181-205.

Fraj-Andrés, E., Herrando, C., Lucia-Palacios, L., & Pérez-López, R. (2023). Intention versus behaviour: integration of theories to help curb food waste among young Spanish consumers. *British Food Journal*, *125*(2), 570-586.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 51-90.

Godey, B., Manthiou, A., Pederzoli, D., Rokka, J., Aiello, G., Donvito, R., & Singh, R. (2016). Social media marketing efforts of luxury brands: Influence on brand equity and consumer behavior. *Journal of Business Research*, *69*(12), 5833-5841.

Grosso, M., Castaldo, S., Li, H. A., & Larivière, B. (2020). What information do shoppers share? The effect of personnel-, retailer-, and country-trust on willingness to share information. *Journal of Retailing*, *96*(4), 524-547.

Guo, X., Zhang, X., & Sun, Y. (2016). The privacy–personalization paradox in mHealth services acceptance of different age groups. *Electronic Commerce Research and Applications*, *16*, 55-65.

Gupta, R., Jain, K., & Jajodia, I. (2021). Determinants of smart speaker adoption intention: extending the theory of planned behaviour. *International Journal of Technology Marketing*, *15*(2-3), 181-202.

Han, S., & Yang, H. (2018). Understanding adoption of intelligent personal assistants: A parasocial relationship perspective. *Industrial Management & Data Systems*, *118*(3), 618-

636.Hayes AF (2017) Introduction to mediation, moderation, and conditional process analysis: A regression-based approach. Guilford publications London.

Hayes, J. L., Brinson, N. H., Bott, G. J., & Moeller, C. M. (2021). The influence of consumer–brand relationship on the personalized advertising privacy calculus in social media. *Journal of Interactive Marketing*, *55*(1), 16-30.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*, 115-135.

Hepler, J., & Albarracin, D. (2014). Liking more means doing more. *Social Psychology*.

Holtrop, N., Wieringa, J. E., Gijsenberg, M. J., & Verhoef, P. C. (2017). No future without the past? Predicting churn in the face of customer privacy. *International Journal of Research in Marketing*, *34*(1), 154-172.

Huang, T. L. (2018). Creating a commercially compelling smart service encounter. *Service Business*, *12*(2), 357-377.

Jung, A. R. (2017). The influence of perceived ad relevance on social media advertising: An empirical examination of a mediating role of privacy concern. *Computers in Human Behavior*, *70*, 303-309.

Kang, H., & Jung, E. H. (2021). The smart wearables-privacy paradox: A cluster analysis of smartwatch users. *Behaviour & Information Technology*, *40*(16), 1755-1768.

Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS quarterly*, 183-213.

Karyda, M., Gritzalis, S., Park, J. H., & Kokolakis, S. (2009). Privacy and fair information practices in ubiquitous environments: Research challenges and future directions. *Internet Research*, *19*(2), 194-208.

Kim, D., Park, K., Park, Y., & Ahn, J. H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, *92*, 273-281.

Kim, M. S., & Kim, S. (2018). Factors influencing willingness to provide personal information for personalized recommendations. *Computers in Human Behavior*, *88*, 143-152.

Kim, S. Y., Kim, J. U., & Park, S. C. (2017). The effects of perceived value, website trust and hotel trust on online hotel booking intention. *Sustainability*, *9*(12), 2262.

Klaus, P., & Zaichkowsky, J. (2020). AI voice bots: a services marketing research agenda. *Journal of Services Marketing*, *34*(3), 389-398.

Klumpe, J., Koch, O. F., & Benlian, A. (2020). How pull vs. push information delivery and social proof affect information disclosure in location based services. *Electronic Markets*, *30*, 569-586.

Krafft, M., Arden, C. M., & Verhoef, P. C. (2017). Permission marketing and privacy concerns—Why do customers (not) grant permissions?. *Journal of Interactive Marketing*, *39*(1), 39-54.

Laaksonen, T., Jarimo, T., & Kulmala, H. I. (2009). Cooperative strategies in customer–supplier relationships: The role of interfirm trust. *International Journal of Production Economics*, *120*(1), 79-87.

Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1-31.

Lee, B. C. (2012). The determinants of consumer attitude toward service innovation–the evidence of ETC system in Taiwan. *Journal of Services Marketing*, *26*(1), 9-19.

Lee, J. M., & Rha, J. Y. (2016). Personalization–privacy paradox and consumer conflict with the use of location-based mobile commerce. *Computers in Human Behavior*, *63*, 453-462.

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems*, *17*(1), 39-71.

Liao, Y., Vitak, J., Kumar, P., Zimmer, M., & Kritikos, K. (2019). Understanding the role of privacy and trust in intelligent personal assistant adoption. In *Information in Contemporary Society: 14th International Conference, iConference 2019, Washington, DC, USA, March 31–April 3, 2019, Proceedings 14* (pp. 102-113). Springer International Publishing.

Libaque-Sáenz, C. F., Wong, S. F., Chang, Y., & Bravo, E. R. (2021). The effect of Fair information practices and data collection methods on privacy-related behaviors: A study of Mobile apps. *Information & Management*, *58*(1), 103284.

Lin, X., & Wang, X. (2020). Examining gender differences in people‘s information-sharing decisions on social networking sites. *International Journal of Information Management*, *50*, 45-56.

Lucia-Palacios, L., & Pérez-López, R. (2021). Effects of home voice assistants' autonomy on instrusiveness and usefulness: direct, indirect, and moderating effects of interactivity. *Journal of Interactive Marketing*, *56*, 41-54.

Makhortykh, M., Urman, A., Gil-Lopez, T., & Ulloa, R. (2022). To track or not to track: examining perceptions of online tracking for information behavior research. *Internet Research*, *32*(7), 260-279.

Mazurek, G., & Małagocka, K. (2019). Perception of privacy and data protection in the context of the development of artificial intelligence. *Journal of Management Analytics*, *6*(4), 344-364.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, *13*(3), 334-359.

McLean, G., & Osei-Frimpong, K. (2019). Hey Alexa… examine the variables influencing the use of artificial intelligent in-home voice assistants. *Computers in Human Behavior*, *99*, 28-37.

Mesch, G. S. (2012). Is online trust and trust in social institutions associated with online disclosure of identifiable information online?. *Computers in Human Behavior*, *28*(4), 1471-1477.

Michler, O., Decker, R., & Stummer, C. (2020). To trust or not to trust smart consumer products: a literature review of trust-building factors. *Management Review Quarterly*, *70*, 391-420.

Moriuchi, E. (2019). Okay, Google!: An empirical study on voice assistants on consumer engagement and loyalty. *Psychology & Marketing*, *36*(5), 489-501.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100-126.

Nunnally, J. C. (1978). *Psychometric Theory: 2d Ed*. McGraw-Hill.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS quarterly*, 105-136.

Manser Payne, E. H., Dahl, A. J., & Peltier, J. (2021). Digital servitization value co-creation framework for AI services: a research agenda for digital transformation in financial service ecosystems. *Journal of Research in Interactive Marketing*, *15*(2), 200-222.

Pitardi, V., & Marriott, H. R. (2021). Alexa, she's not human but… Unveiling the drivers of consumers' trust in voice-based artificial intelligence. *Psychology & Marketing*, *38*(4), 626-642.

Schaupp, L. C., & Carter, L. (2010). The impact of trust, risk and optimism bias on E-file adoption. *Information Systems Frontiers*, *12*, 299-309.

Singh, J., & Sirdeshmukh, D. (2000). Agency and trust mechanisms in consumer satisfaction and loyalty judgments. *Journal of the Academy of marketing Science*, *28*, 150-167.

Smit, E. G., Van Noort, G., & Voorveld, H. A. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Hhuman Nehavior*, *32*, 15-22.

Tan, W. K., & Liao, P. H. (2021). What triggers usage of gift-giving apps? A comparison between users and non-users. *Service Business*, *15*(3), 515-538.

Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior*, *93*, 1-12.

Van Pinxteren, M. M., Wetzels, R. W., Rüger, J., Pluymaekers, M., & Wetzels, M. (2019). Trust in humanoid robots: implications for services marketing. *Journal of Services Marketing*, *33*(4), 507-518.

Vimalkumar, M., Sharma, S. K., Singh, J. B., & Dwivedi, Y. K. (2021). ‗Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior*, *120*, 106763.

Volchek, K., Yu, J., Neuhofer, B., Egger, R., & Rainoldi, M. (2021). Co-creating personalised experiences in the context of the personalisation-privacy paradox. In *Information and Communication Technologies in Tourism 2021: Proceedings of the ENTER 2021 eTourism Conference, January 19–22, 2021* (pp. 95-108). Springer International Publishing.

Wang, X. W., Cao, Y. M., & Park, C. (2019). The relationships among community experience, community commitment, brand attitude, and purchase intention in social media. *International Journal of Information Management*, *49*, 475-488.

Wu, B., & Chen, X. (2017). Continuance intention to use MOOCs: Integrating the technology acceptance model (TAM) and task technology fit (TTF) model. *Computers in Human Behavior*, *67*, 221-232.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*(1), 42-52.

Yang, H., & Lee, H. (2019). Understanding user behavior of virtual personal assistant devices. *Information Systems and e-Business Management*, *17*, 65-87.

Yuan, Y., Lai, F., & Chu, Z. (2019). Continuous usage intention of Internet banking: a commitment-trust model. *Information Systems and e-Business Management*, *17*, 1-25.

Zimmer, J. C., Arsal, R. E., Al-Marzouq, M., & Grover, V. (2010). Investigating online information disclosure: Effects of information relevance, trust and risk. *Information & Management*, *47*(2), 115-123.

## APPENDIX 2.

**Appendix 2.1.** Measures

| Latent variable | Items |
|---|---|
| The perceived value of personalisation | VALUE1: I think the benefits gained from receiving personalised information from my smart home speaker can offset the risks of my information disclosure.<br>VALUE2: The value I gain from receiving personalised information from my smart home speaker is worth the information I give away.<br>VALUE3: I think the risks of my information disclosure will be greater than the benefits gained from receiving personalised information from my smart home speaker. |
| Trust | TRUST1: Smart speaker providers are trustworthy.<br>TRUST2: Smart speaker providers treat my personal information fairly and honestly.<br>TRUST3: I trust that smart speaker providers have my best interests in mind when dealing with my information.<br>TRUST4: I can trust the privacy policy of smart speaker providers. |
| Attitude toward covert information collection | COVERT1: I think using covert strategies like covert data collection is a good information collection system.<br>COVERT2: The fact that my smart home speaker collects data without my awareness / without my knowledge makes me feel good.<br>COVERT3: I prefer the speaker not constantly request permission to collect data.<br>COVERT4: I like the idea that the smart home speaker is capturing information even though I am not actively using it. |
| Attitude toward overt information collection | OVERT1: I think using overt strategies like overt data collection is a good information collection system.<br>OVERT2: The fact that my smart home speaker collects data with my awareness / with my knowledge makes me feel good.<br>OVERT3: I prefer the speaker constantly requests permission to collect data.<br>OVERT4: I like the idea that the smart home speaker captures information only when I am actively using it. |
| Intention to continue to use | CONT1: I will frequently use the smart speaker in the future.<br>CONT2: I intend to continue using the smart speaker rather than discontinue its use.<br>CONT3: I will use the smart speaker regularly in the future. |

# CHAPTER III

## CAN THE HUMANISATION OF SMART HOME SPEAKERS IMPROVE USERS‘ ATTITUDE TOWARD COVERT INFORMATION COLLECTION?

## 3.1. INTRODUCTION

Covert information collection represents not only a risk to the privacy of users but also a danger to the image of companies, whose reputation and trust may be compromised. According to a study conducted by Morey et al. (2015), only 27% of the people surveyed were aware that they were sharing their friends list and only 18% were aware that their communications history was being shared. Likewise, in research by Turow et al. (2015) 58% of respondents said they have little control over what companies can learn about them from the information they collect. Therefore, more attention should be paid to users‘ attitude toward covert information collection.

Frick et al. (2021) defined surveillance effect as ‒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‖. Information collection by smart home speakers includes any oral information the user provides, and is collected by companies through microphones. They have a physical button to switch off the microphones. These devices should only record and listen after the wake-up word to provide the user with the information he/she has requested. This is how the devices should work. However, consumers often feel they are being continuously spied on (Frick et al., 2021; Lau et al., 2018; Siddike et al., 2018), experience privacy concerns and stress, and show discomfort with this covert information strategy (Benlian et al., 2019; Song et al., 2022). Consumers are afraid about the data collected and some of them turn off the device before having private conversations to avoid unwanted surveillance (Siddike et al., 2018).

Similarly, as consumers perceive that are being surveyed, they may also think that companies use covert information collection, not having a positive attitude toward this type of strategy. This outcome variable is very important because a better attitude

toward covert information collection means that companies can provide personalised messages without asking for permission at each interaction. It is also important for customer experience, since interruptions during the interaction may reduce customer flow. Recent research has examined perceived surveillance, its antecedents (Frick *et al.*, 2021) and consequences (Plangger and Montecchi, 2020), suggesting that trust in the device is the main factor to reduce perceived surveillance (Frick et al., 2021). However, extant studies have not considered what characteristics of smart home speakers can reduce perceived surveillance, nor how to improve consumer attitudes toward covert information collection.

Based on parasocial relationship theory (PSR), research has concluded that humanisation enhances the credibility of messages (Foehr and Germelmann, 2020; Poushneh, 2021) and increases social presence during the interaction process (Kang and Kim, 2022; Toader et al., 2019), generating trustworthy and close relationships akin to those that arise between friends (Han and Yang, 2018; Pitardi and Marriott, 2021). On the other hand, under the framework of uncanny valley theory and contrary to the above findings, Lavado-Nalvaiz et al. (2022) recently found that humanisation can diminish perceived privacy risks for low levels of humanisation, while high levels increase perceived risks of information disclosure. Nevertheless, we still do not know whether humanising smart home speakers helps to reduce the effects of perceived surveillance, and whether humanisation can improve consumers‘ attitude toward covert information collection.

The present research has three aims. First, it analyses humanisation as a factor to improve users‘ attitude toward covert information collection by increasing trust and social presence and by reducing perceived surveillance. Second, it analyses the mediating role of trust in the relationship between humanisation and users‘ attitude

toward covert information collection. Finally, it examines how social presence can reduce users‘ perceived surveillance. To achieve these objectives, 679 American smart home speaker users are surveyed, and their responses are analysed using structural equation modelling (SEM).

This chapter contributes to previous research in several ways. First, this study contributes to interactive research by examining the antecedents of a new outcome variable: attitude toward covert information collection. Second, the chapter contributes to anthropomorphism and uncanny valley theory research by providing new evidence of how humanisation helps improve social presence and users‘ attitude toward covert information collection by these devices, and to reduce perceived surveillance. Finally, this study contributes to extant research on interactive and smart products by providing empirical evidence of the important role that social presence plays in improving users‘ behaviour, particularly reducing users‘ perceived surveillance, improving users‘ attitude toward covert information collection and demonstrating that humanisation can generate trust in the service provider through social presence.

## 3.2. CONCEPTUAL DEVELOPMENT

### 3.2.1. Humanisation

Users who interact with devices that have anthropomorphic attributes may feel that they are interacting with another human being rather than a machine (Pitardi and Marriot, 2021). Regarding smart home speakers, research has mainly focused on conversational features, such as type of voice (Chen et al., 2022) or sense of humour (Go and Sundar, 2019; Kang and Kim, 2022). Two theories have been advanced to

explain the effects that humanisation has on users‘ behaviours and emotions: realism maximisation theory (Groom et al., 2009) and uncanny valley theory (Mori, 1970).

Realism maximisation theory states that human personality characteristics trigger positive emotional reactions in consumers as they perceive that they are interacting with another human being (Lee and Oh, 2021). Humanisation enables smart devices to generate higher levels of trust, feelings of familiarity and social presence (Foehr and Germelmann, 2020), and can even create an environment that generates high levels of user self-disclosure (Rhim et al., 2022).

On the other hand, uncanny valley theory, proposed by Mori (1970), has been used to explain the relationship between the degree of humanisation of an object and users‘ emotional response when using it. According to this theory, humanisation has a cubic effect on users‘ emotional response. Thus, low but increasing levels of humanisation can generate affinity toward the device, until a point of humanisation at which the device starts to be perceived as creepy and upsetting, leading to negative emotions of distress and eeriness (Mathur et al., 2020). When humanisation is so high that consumers believe they are talking to a human being, the effect of humanisation on consumers‘ feelings becomes positive once more (Mathur et al., 2020). Although users may perceive some smart devices to be highly humanised, they will never mistake them for human beings as their physical aspect differs. Previous research has found that humanisation exerts such a quadratic effect on user behaviour, i.e., user perceived risks (Lavado-Nalvaiz et al., 2022). This is because a voice that sounds human but is actually being generated by a computer may cause confusion over the humanness of the device and cause distrust toward it (Xie et al., 2020).

### 3.2.2. Social presence

With the increasing development of technology, PSR theory has been employed in various studies on the interaction between individuals and non-human entities (Han and Yang, 2018; Tsai et al., 2021). Heerink et al. (2010) conceptualised social presence as the degree to which a machine can make a human being feel as if they are interacting with another individual. In the present study, social presence is defined as the feeling of human contact, human sociability and human sensitivity; in essence, the feeling of interacting with a real person when using a smart home speaker.

Smart home speakers can imitate human attributes, such as the ability to communicate verbally, by providing with human responses, such as jokes and original answers, or can even have a ‒human‖ name (Go and Sundar, 2019). Once the voice assistant is perceived as being close to human, users engage in interpersonal social interactions and develop a parasocial relationship with it (Han and Yang, 2018). Feelings of closeness, trust and friendliness then emerge, which in turn generates regularity in interaction (Ki et al., 2020) and a better attitude toward the device (Pitardi and Marriot, 2021). However, there is a need to further study social presence and how it is perceived by users in terms of their attitudes toward covert information collection and whether social presence can help reduce perceived surveillance.

### 3.2.3. Attitude toward covert information collection

As mentioned in chapter 1, previous research has found that covert strategies also increase the perceived risk regarding the use of information. Users feel a sense not only of invasion and loss of privacy but also of perceived control over their data (Libaque-Sáenz et al., 2021). In this chapter, we focus on user‘s attitude toward that type of strategy. Following previous research on technology adoption and use, we

define this attitude as the user‘s positive or negative beliefs about such type of information collection by the smart speaker (Bajaj and Nidumolu, 1998). Ho et al. (2022) studied the attitude toward non-conscious data collection among Generation Z. They found that 50% of consumers were not worried about covert data collection by firms, and thus concluded that users have a neutral attitude toward that collection strategy. A possible explanation for this result is that young consumers are resigned with respect to data sharing, and accept data collection as inevitable. Similarly, Lau et al. (2018) found that users of the devices do not feel uncomfortable with an ―always listening‖ device because the recordings will not be of interest for the firm or because firms have already collected users‘ private information, so the new information collected is just a small addition. The present research augments previous studies by focusing on a concrete smart product and including not only age and sex variables, but also trust and humanisation, as antecedents of attitude toward covert information collection.

### 3.2.4. Perceived surveillance

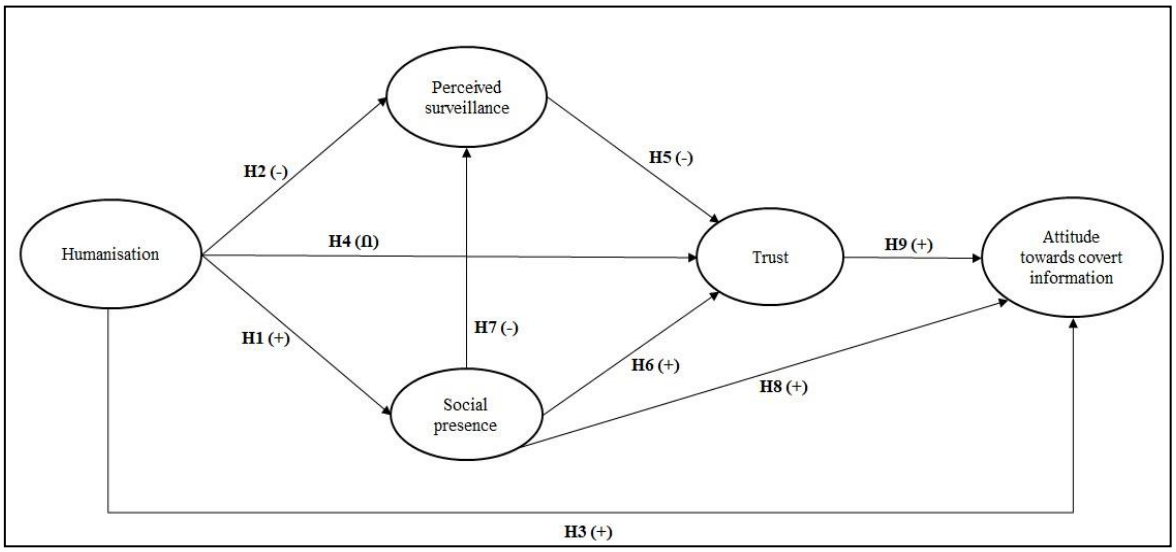
Surveillance involves the acquisition of customers‘ personal data by companies (Plangger and Montecchi, 2020). Smart home speakers need to continuously analyse audio signals as they wait to receive their activation messages (e.g., ―OK Google‖ or ―Hey Alexa‖), and are technically capable of recording audio and transmitting it to a server (Frick et al., 2021). Lau et al. (2018) made a qualitative research about the users‘ perception of how smart speakers work. They found that users do not know if the device is recording or listening all the time. Some previous research based on interviews pointed out that consumers have fear about the data collected and that some turned off the device before having private conversations to avoid unwanted surveillance (Siddike et al., 2018). They showed that users are afraid of being listened to, increasing user‘s

feelings of stress (Benlian et al., 2019) and reducing the perceived value of smart home speakers and the intention to use them (Kowalczuk, 2018).

### 3.3. HYPOTHESIS DEVELOPMENT

The theoretical model and research hypotheses are presented in this section. The model proposed and the hypotheses to be tested are shown in Figure 3.1.

**Figure 3.1.** Theoretical model




Previous research has considered how anthropomorphic design features of smart devices and robots affect users‘ perceptions of social presence (Rhim et al., 2022: Toader et al., 2019). When interacting with smart devices that have anthropomorphic features, such as humanlike voices and manners of responding, people may come to believe that they are interacting with another human being, enhancing feelings of social presence (Kang and Kim, 2022). According to PSR theory, if users interact and socialise with smart devices in a similar way as they would do with humans they develop feelings of closeness and intimacy. Blut et al., (2021) proposed that by giving robots humanlike features, people perceived that they are connecting with another human being. Therefore, we propose:

**H1.** *Humanisation of smart home speakers has a positive effect on social presence.*

Anthropomorphism may reduce privacy concerns derived from consumers‘ perceived surveillance when using smart speakers. When technology possesses anthropomorphic characteristics, the sense of privacy invasion is reduced (Benlian et al., 2019). Recently, Lucia-Palacios and Pérez-López (2023) asserted that interactivity helps to decrease the perception of smart home speakers‘ intrusiveness. Interactivity involves bidirectional communication and responsiveness – two aspects of natural language and anthropomorphism included in smart home speakers. In addition, Blut et al., (2021) demonstrated that anthropomorphism has a positive effect on the perception of privacy security, suggesting that the more humanised a robot is, the safer the robot is considered to be in terms of privacy risks and privacy invasion. Thus, we propose:

**H2.** *Humanisation of smart home speakers has a negative effect on perceived surveillance.*

According to PSR theory, people are more likely to experience feelings of familiarity, intimacy and closeness when interacting with a device if it is perceived as having humanlike features (Blut et al., 2021; Poushneh 2021). Such features create a climate of comfort that leads users to relax and be less worried about the possibility of smart home speakers collecting information covertly. This can lead them to have a more favourable attitude toward this type of information collection. Furthermore, Melumad and Meyer (2020) stated that if devices are perceived as friends, users will voluntarily disclose information even without being subject to a prior request for permission. This is because a feeling of psychological comfort is created between user and device. Hence, we propose:

**H3.** *Humanisation of smart home speakers has a positive effect on attitude toward covert information collection.*

Under maximisation realism theory, providing a humanlike mind to an artificial device causes users to perceive it as a more competent agent (Waytz et al., 2010). Indeed, trust improves when the intelligent agent applies humanlike characteristics, such as not interrupting during the interaction, being patient or even making jokes (Go and Sundar, 2019).

According to uncanny valley theory, humanisation can lead to increased trust feelings and social presence toward the device, brand or firm (Foehr and Germelmann, 2020; Poushneh, 2021). However, over-humanisation can raise major concerns, as users may be confused by an artificial voice that resembles that of a human, creating doubts about its humanity. These feelings can result in the user distrusting the smart home speaker, which also increases distrust of the provider behind the device (Xie et al., 2020). Following recent findings in the field of smart speakers (Lavado-Nalvaiz et al., 2022), we follow this theory. Thus, we propose:

**H4.** *Humanisation of smart home speakers has an inverted U-shaped effect on trust.*

Privacy intrusion is annoying and irritating (Krafft et al., 2017), and the problem is particularly salient when smart home speakers collect information without consumer awareness (Frick et al., 2021; Jung et al., 2021). Most of the time, users are unaware of the amount of personal information smart home speakers are processing, and when they are doing so. These concerns make users feel that they have no control of what information is disclosed (Klumpe et al., 2020), in turn risking customer relationships and even generating feelings of distrust (Plangger and Montecchi, 2020). Thus, we propose:

**H5.** *Perceived surveillance has a negative effect on trust.*

Pitardi and Marriott (2021) demonstrated that social presence enhances consumer trust toward a device. However, it remains unclear whether social presence when interacting with a smart product can also create trust in the service provider. Moreover, some studies have shown that chatbots improve trust in affiliated websites. This is because they show signs of social presence, which is key in building trust in the avatar and consequently in the website (Foster et al., 2022). Parasocial interactions between the smart home speaker and the user enhance the user‘s trust (Hsieh and Lee, 2021). Based on this, we propose that the trust generated by the social presence of the device applies not only to the product but also to the brand or the service provider. Thus, we propose:

**H6.** *Social presence of smart home speakers has a positive effect on trust.*

When users interact with smart home speakers in the same way as they would with human beings, users experience feelings of closeness and intimacy toward the devices. Benlian et al. (2019) proposed that humanisation increases feelings of closeness with devices, such that users may be less concerned about the information they are providing to the device and the risks arising from that disclosure. Ki et al. (2020) showed that the social presence of smart home speakers influences users‘ self-disclosure, reducing privacy risks and perceptions of surveillance. Thus, we propose:

**H7:** *Social presence of smart home speakers has a negative effect on perceived surveillance.*

Tsai et al. (2021) suggested that the intuitive perception of being in the presence of another smart being triggers a sense of interpersonal interaction. When users perceive

that they are dealing with a real person rather than with an electronic device, their perceived risk regarding the information that is disclosed is reduced (Ki et al. 2020; Melumad and Meyer, 2020). In fact, it is possible that even more information will be revealed because they see the speaker as a friend with whom they can socialise. As the device becomes more familiar with the user, these feelings of closeness and intimacy increase. Thus, users may show lower privacy concerns and a better attitude toward covert information collection. Therefore, we propose:

**H8.** *Social presence of smart home speakers has a positive effect on attitude toward covert information collection.*

Trust in the service provider can be defined as the degree to which a company can be trusted to protect users‘ personal information (Bawack *et al.*, 2021). Therefore, trust in the service provider will play a key role in making consumers feel more confident about sharing their personal information (Schaupp and Carter, 2010), and will positively influence users‘ attitude toward using artificial intelligence (AI) such as voice-based assistants (Hsieh and Lee 2021; Pitardi and Marriott 2021). Furthermore, chapter 2 has already demonstrated a positive relationship between trust and attitude toward covert information collection. Therefore, we propose:

**H9.** *Trust in the service provider has a positive effect on attitude toward covert information collection.*

### 3.4. METHODOLOGY

We used the same data as in chapter 2, obtained through a survey conducted via Amazon Mechanical Turk. Like in that chapter, the sample was formed by 679 American participants over 18 years old and who owned a smart home speaker.

The constructs and scales were presented randomly so participants could not guess what our intentions were. The items of the selected variables are based on constructs used in previous research, all of which are reflective (Appendix 3.1), and measured using a seven-point Likert scale (1 = ‒completely disagree‖ to 7 = ‒completely agree‖). The independent variable, humanisation, is composed of five items based on previous research (Epley et al., 2007; Lu et al., 2019). Social presence was measured using five items proposed by Pitardi and Marriott (2021). Perceived surveillance consisted of four items adapted from Jung et al. (2021). Trust in the service provider was adapted from Lee and Rha (2016). Finally, we adopted the attitude construct used by Lee (2012), which consists of four items taken from the definition of covert strategy proposed by Aguirre et al. (2015).

Additionally, control variables are included. Age was an open-ended response; education was formed of four levels; gender was a dummy variable (male = 1, female = 0); and frequency of use was also a categorical variable comprising five levels.

### 3.4.1. Descriptive results

Similar to the previous chapter**,** this section describes the characteristics of the sample of the present study (see Table 3.1), that are the same as the previous one. Of the respondents, 55.52% were women; 56.55% were aged between 25 and 34; and 61.86% had a higher level of education (i.e., they held a bachelor‘s degree). In terms of average income level, 46.84% earned between $40,000 and $79,999 per year, which is considered a mid-level income. Finally, regarding the brand used, 65.87% used Alexa, 23.27% Google Home, 9.79% Home Pod (Apple) and 1.07% Cortana (Microsoft).

**Table 3.1.** Sample characteristics

| Gender(%) | | Education(%) | | Frequency(%) | | Brand(%) | | Income $ (%) | | Age(%) | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| F | 55.52 | N | 1.03 | N | 0.44 | Alexa | 65.87 | <20,000 | 5.30 | 18–24 | 3.09 |
| M | 44.48 | C | 7.36 | AN | 1.62 | Cortana | 1.07 | 20,000–39,999 | 11.93 | 25–34 | 56.55 |
| | | B | 61.86 | S | 17.38 | Google | 23.27 | 40,000–59,999 | 24.45 | 35–44 | 23.71 |
| | | M/PHD | 29.75 | AED | 50.66 | HomePod | 9.79 | 60,000–79,999 | 22.39 | 45–54 | 10.75 |
| | | | | ED | 29.99 | | | 80,000–99,999 | 23.56 | 55–64 | 4.27 |
| | | | | | | | | >100,000 | 12.08 | >65 | 1.62 |
| | | | | | | | | Not disclosed | 0.29 | | |

***Note**: F=Female; M=Male; N=None; C=College; B=Bachelor's; M/PHD=Master's/PhD; N=Never; AN=Almost never; S=Sometimes; AED=Almost every day; ED=Every day.*

## 3.5. RESULTS

### 3.5.1. Common method bias

To avoid common method bias related to the survey or questionnaire design, the researchers pointed out to the respondents that all responses were anonymous and that there were no correct answers (MacKenzie and Podsakoff, 2012). Questions and items were randomly ordered in the survey to hide the researchers' interest and conceal the relationship between dependent and independent variables. This ensured the two variable types were psychologically separated (Podsakoff et al., 2012). Additionally, Harmon's one-factor test was performed on the entire sample in order to control for the possible existence of common method bias. The results showed that one factor explained 19.80% of the variance. When the rest of the factors of the model were incorporated, the variance explained increased to 78.32%, confirming that there was no common method bias. The model was run using a new _random' variable (a single-indicator latent variable) to obtain the variance inflation factor (VIF) values of all model variables (Kock and Lynn, 2012). The results show that the VIF values are equal to or lower than 3.3, so the model can be considered free of common method bias (see Table 3.2).

### 3.5.2. Measurement model validation

As we used latent variables in this study, it was necessary to confirm the unidimensionality of the constructs by conducting exploratory factor analysis. For this purpose, SPSS software was used, and five constructs were obtained. SEM and PLS combine two statistical methods: confirmatory factor analysis and path analysis.

Confirmatory factor analysis aims to identify the validity of the latent variables. Path analysis is used to find the causal relationships among variables. Confirmatory factor analysis includes testing the internal consistency of the latent variables (using Cronbach‘s alpha, the composite reliability index, convergent validity analysis and discriminant validity analysis). As for the factor loadings, all constructs were above 0.7 – the minimum acceptable value (Carmines and Zeller, 1979) (see Table 3.2). SmartPLS4 was used to carry out this analysis.

**Table 3.2.** Items and measurement model

| | VIF | Loadings | Cronbach's alpha | Composite reliability | AVE |
|---|---|---|---|---|---|
| **Humanisation** | 1.64 | | 0.963 | 0.971 | 0.871 |
| HUMAN1 | | 0.910 | | | |
| HUMAN2 | | 0.938 | | | |
| HUMAN3 | | 0.944 | | | |
| HUMAN4 | | 0.940 | | | |
| HUMAN5 | | 0.935 | | | |
| **Social presence** | 1.73 | | 0.888 | 0.918 | 0.691 |
| SOCPR1 | | 0.748 | | | |
| SOCPR2 | | 0.854 | | | |
| SOCPR3 | | 0.862 | | | |
| SOCPR4 | | 0.847 | | | |
| SOCPR5 | | 0.842 | | | |
| **Surveillance** | 2.69 | | 0.859 | 0.905 | 0.704 |
| SURV1 | | 0.828 | | | |
| SURV2 | | 0.833 | | | |
| SURV3 | | 0.877 | | | |
| SURV4 | | 0.816 | | | |

**Table 3.2. (Continued).** Items and measurement model

| | VIF | Loadings | Cronbach's alpha | Composite reliability | AVE |
|---|---|---|---|---|---|
| **Trust** | 2.15 | | 0.902 | 0.932 | 0.773 |
| TRUST1 | | 0.891 | | | |
| TRUST2 | | 0.882 | | | |
| TRUST3 | | 0.876 | | | |
| TRUST4 | | 0.867 | | | |
| **Att covert information collection** | 2.22 | | 0.946 | 0.961 | 0.861 |
| COVERT1 | | 0.939 | | | |
| COVERT2 | | 0.923 | | | |
| COVERT3 | | 0.918 | | | |
| COVERT4 | | 0.932 | | | |

The internal consistency of the latent variables was then analysed. The Cronbach's alpha and composite reliability index were above the minimum standards, in this case 0.7 (Nunnally, 1978). All latent variables presented average variance extracted (AVE) values over 0.5 (Fornell and Larcker, 1981) and over 0.6 (Hair et al., 2014), confirming the convergent validity of the measurement model. The discriminant validity of the model was also confirmed, since the heterotrait–monotrait (HTMT) ratios were below 0.85 (Henseler et al., 2015), as shown in Table 3.3.

**Table 3.3.** Discriminant validity

| | COVERT | HUMAN | SOCPRES | SURV | TRUST |
|---|---|---|---|---|---|
| **COVERT** | **0.928** | 0.545 | 0.501 | -0.268 | 0.357 |
| **HUMAN** | 0.572 | **0.933** | 0.412 | -0.483 | 0.395 |
| **SOCPRES** | 0.541 | 0.440 | **0.832** | -0.112 | 0.367 |
| **SURV** | 0.297 | 0.529 | 0.133 | **0.839** | -0.292 |
| **TRUST** | 0.385 | 0.424 | 0.408 | 0.330 | **0.879** |

***Note**: Square roots of AVE appear in bold. Below the bold diagonal appear correlations between variables. Above appear HTMT ratio values. COVERT=Attitude covert information collection; HUMAN=Humanisation; SOCPRES=Social presence; SURV=Perceived surveillance; TRUST=trust.*

### 3.5.3. Hypothesis testing

SmartPLS4 software was used to estimate the model, providing the path coefficients and their level of significance. The authors have examined the predictive

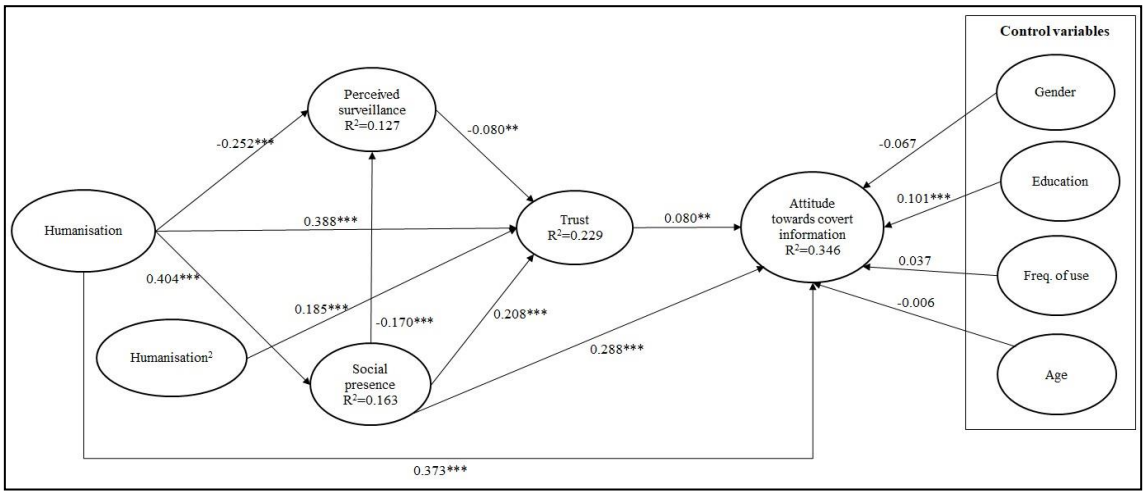
performance of the model ($Q^2$), which is used as a goodness-of-fit criteria according to Stone (1974) and Geisser (1974). Positive values indicate good model performance. The results showed that the $Q^2$ measures were adequate.

The results (see Figure 3.2) suggest that humanisation has a direct, positive and significant effect on social presence, which supports H1. As there is a negative and significant relationship between humanisation and perceived surveillance, H2 is also supported. Humanisation has a direct, positive and significant effect on attitude toward covert information collection, supporting H3. Regarding humanisation and trust, a significant quadratic effect of humanisation on trust exists ($b=0.185$, $p<0.05$). However, Figure 3.3 shows that humanisation has a U-shaped effect on trust, which does not support H4. Specifically, humanisation influences trust negatively when it is low; however, for greater levels of humanisation the effect becomes positive.

Social presence has a positive and significant effect on trust, and perceived surveillance has a negative and significant effect on trust, supporting H5 and H6, respectively. The results show that social presence significantly and negatively affects perceived surveillance, which also supports H7. Additionally, social presence and trust have positive effects on having a positive attitude toward covert information collection, supporting H8 and H9.

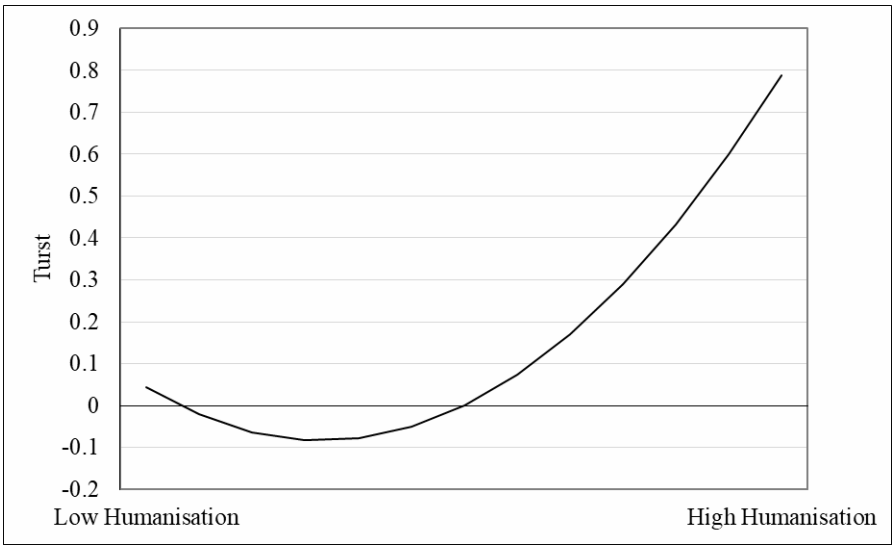
Regarding the control variables, only level of education shows a positive and significant effect on attitude toward covert information collection. This means that those with a higher level of education have a better attitude toward covert information collection.

**Figure 3.2.** Structural model results




***Note**: ***significant at 1%; **significant at 5%; *significant at 10%*

**Figure 3.3.** Quadratic effect of humanisation on trust




Although no mediation hypothesis has been proposed in this chapter, we consider it instructive to point out the existing mediating effects (Table 3.4). The results indicate that both social presence and perceived surveillance partially mediate the relationship between humanisation and trust in the service provider. Trust is also found to play a mediating role between humanisation and attitudes toward covert information collection. However, it should be noted that social presence has the greatest mediating effect between these two variables.

**Table 3.4. Mediating effects**

| | Point estimate | t-tatistic | p-value | Lower | Upper |
|---|---|---|---|---|---|
| HUMAN→TRUST→COVERT | 0.051 | 3.143 | 0.002 | 0.020 | 0.082 |
| HUMAN →SURV→TRUST | 0.020 | 1.866 | 0.062 | 0.000 | 0.044 |
| **HUMAN →SOC PRES→SURV** | **-0.069** | **3.923** | **0.000** | **-0.106** | **-0.037** |
| **HUMAN → SOC PRES→TRUST** | **0.085** | **4.235** | **0.000** | **0.048** | **0.127** |
| HUMAN2 → TRUST → COVERT | 0.024 | 2.451 | 0.014 | 0.008 | 0.047 |
| HUMAN→SURV→TRUST →COVERT | 0.003 | 1.447 | 0.148 | 0.000 | 0.007 |
| **HUMAN→SOC PRES→TRUST→COVERT** | **0.011** | **2.228** | **0.026** | **0.003** | **0.023** |
| HUMAN→SOC PRES→SURV→TRUST | 0.006 | 1.674 | 0.095 | 0.000 | 0.013 |
| HUMAN→SOC PRES→SURV→TRUST→COVERT | 0.001 | 1.360 | 0.174 | 0.000 | 0.002 |
| SOC PRES→SURV→TRUST | 0.014 | 1.731 | 0.084 | 0.000 | 0.031 |
| SOC PRES→TRUST→COVERT | 0.028 | 2.307 | 0.021 | 0.008 | 0.055 |
| SOC PRES→SURV→TRUST→COVERT | 0.002 | 1.390 | 0.165 | 0.000 | 0.005 |
| SURV→TRUST→COVERT | -0.011 | 1.538 | 0.124 | -0.026 | -0.000 |

***Note**:COVERT=Attitude toward covert information collection; HUMAN=Humanisation; HUMAN2=Humanisation quadratic effect; SOCPRES=Social presence; SURV=Perceived surveillance; TRUST=trust.*

## 3.6. DISCUSSION

The results show that humanisation is positively related to social presence, confirming the findings of previous studies (Toader et al., 2019; Kang and Kim, 2022; Rhim et al., 2022) and in line with PSR theory. This implies that providing smart home speakers with a humanlike tone of voice, NLP ability or personality increases users‘ feelings that they are in relationship with another person rather than with an artificial device. Furthermore, in line with previous authors (Benlian et al., 2019), it is confirmed that humanisation helps to reduce perceived surveillance while simultaneously improving users‘ attitude toward information collection.

The results show that humanisation has a U-shaped effect on trust in the service provider. This implies that low levels of humanisation have a negative influence on trust, up to a point at which when humanisation increases, trust increases. It should be noted that the negative effect is very small and only happens for low levels of

humanisation, while the positive effect is much more notable. This leads us to suggest that higher levels of humanisation are more beneficial, which contradicts our expectations. We can propose several possible explanations for this surprising effect. First, previous research has shown that, depending on the humanisation features, the results may be contradictory. The features presented by smart home speakers typically offer few options to include human-like characteristics, and they will never be mistaken for humans in terms of anthropomorphic appearance (Lavado-Nalvaiz et al., 2022). A second explanation is that consumers may have gained familiarity with smart home speakers. As a result, greater familiarity with these devices may involve that medium levels of humanisation are less likely to create feelings of eeriness and discomfort, which may explain why the humanisation-trust link does not follow an inverted U-shaped effect (Zlotowski et al., 2015). Nevertheless, Reis et al. (2011) stated that for familiarity to improve the effects of humanisation on likeability, previous interactions should be pleasant. Furthermore, we find that frequency of use of smart home speakers is not relevant to explain attitude toward covert information collection. Thus, the role of familiarity with these devices is still not clear and future research could focus on studying how it can affect trust and attitude toward information collection. Third, the user‘s personal characteristics can modify how they react to humanisation in smart devices, since sensitivity toward privacy risks varies across generations (Van Schaik et al., 2017). Therefore, further research should try to explain the role of humanisation on trust in the context of smart home speakers by investigating these personal characteristics.

As proposed, perceived surveillance reduces trust in the provider. This is consistent with previous research (Bawack et al., 2021; Krafft et al., 2017), and demonstrates that concerns related to privacy cause a decrease in trust. Regarding the

role of social presence, results show that this construct is positively related to trust in the provider. This also aligns with previous findings that smart devices that exhibit humanlike behaviours generate an affinity between people and these devices, building a trusting relationship in this context (Han and Yang, 2018; Pitardi and Marriott, 2021).

The findings also show that social presence is negatively related to perceived surveillance, indicating that when users perceive that they receive social support from smart home speakers, perceptions of surveillance can be reduced (Ki et al., 2020). Furthermore, we confirm that social presence helps to improve users‘ attitude toward information collection, in accordance with previous studies (Melumad and Meyer, 2020). This study also confirms that the influence of humanisation on attitude toward covert information collection is more important through social presence than through trust. For all these reasons, social presence acquires an important role in the model. This is in accordance with previous studies on this topic (Poushneh, 2021), and suggests that social presence feelings may lead users to be less concerned about the information the device is collecting from them and may also reduce those negative feelings of distrust.

Finally, the results show that, per previous studies (Pitardi and Marriott, 2021) and consistent with chapter 2, trust in the service provider plays an important role as it is positively related to users‘ attitude toward covert information collection. This study demonstrates that if users trust the service provider with respect to how their personal information is handled, used and stored, their attitude toward the collection of this information will be positive, even if users may think that the information is collected covertly.

Regarding control variables, people with lower levels of education may have difficulties understanding the technical aspects behind this information collection and

storage strategy, resulting in greater concern about the misuse of their personal data and possible breaches of their privacy (Boerman et al., 2021).

## 3.7. CONCLUSION

### 3.7.1. Theoretical implications

Present research contributes to the literature on interactive and smart products by considering the antecedents of a relevant consumer outcome: attitude toward covert information collection. Asking users‘ permission to collect personal information at each interaction, and thereby interrupting the flow of the conversation, can create a negative customer experience. Although some research has examined intrusiveness (Benlian et al., 2019; Lucia-Palacios and Pérez-López, 2021), little attention has been paid to perceived surveillance and even less to the perception or the attitude toward covert information collection. In line with this contribution, the results reveal the important role of humanisation and social presence in improving users‘ attitude toward covert information collection – which, to our knowledge, has not been previously analysed. Furthermore, both variables reduce users‘ perceived surveillance and increase trust in the service provider. The results contribute to PSR theory by showing that social presence and humanisation reduce some of the risks commonly associated with smart home speakers, such as the feeling of being under surveillance. Little research (Benlian et al., 2019; Lavado-Nalvaiz et al., 2022) has studied the effects of humanisation on negative aspects, such as intrusiveness and privacy risks.

The findings offer further evidence on the effect of humanisation on trust in the context of smart home speakers. This research examines the role of humanisation in building a relationship of trust with the service provider, and shows that humanisation

has a U-shaped effect, suggesting that the more humanisation, the better. This result does not support either realism maximisation theory or uncanny valley theory. Therefore, more research is needed to offer additional insights. Nevertheless, this study provides new results with respect to the link between humanisation and trust in the service provider, since extant studies have only analysed trust in the humanised object, and not in the service provider.

### 3.7.2. Managerial implications

The results of this research show different ways in which marketers and companies can improve users‘ attitude toward covert information. However, there should be a balance between what is ethical and what the company wants to achieve. Collecting as much information as possible is essential to provide a better service, but, at the same time, ethical business practices must be used to set certain limits. This study demonstrates the importance of trust in the service provider in improving users‘ attitude toward covert data collection. Trust can be enhanced in different ways. Intrusive ads should be reduced to reduce perceived surveillance, and a recommendation for designers is to include an option to remind the user that the speaker is on. Informing and being more transparent can help to increase trust.

Similarly, when designing their interfaces, developers of smart home speakers must take into account the degree of humanisation they want to achieve, either through voice or conversation, to ensure greater naturalness when communication is taking place. By incorporating this aspect, social presence will increase and users will perceive that they are interacting with something similar to a human being, which will generate feelings of closeness and reduce perceived surveillance. Therefore, managers should focus on including capabilities that help to increase social presence, mitigating surveillance and improving users‘ attitude toward covert information collection.

These managerial suggestions can be extended to other contexts. For example, consumers are also using voice assistants to search for products online (Gao and Liu, 2022), and on websites in the form of front-line voice bots (Buhalis et al., 2022). All new cars are equipped with voice control systems, which may give rise to the same privacy concerns as with smart home speakers as it is an intimate space. During conversations with voice assistants, consumers may reveal important information for companies, such as brand judgements and emotions about certain brands or products that can be recorded. This is extremely important with the emergence of new IA bots like ChatGPT, Bing or Bard that are used in the business context.

### 3.7.3. Research limitations and future research suggestions

Although this research makes broad theoretical contributions, as well as practical contributions for providers of this technology, it is subject to certain limitations that offer opportunities for future research. This study explained humanisation using a latent variable, so future research could analyse the humanisation variable at different levels, from low to high degrees.

It would be interesting to extend this research to different cultural contexts. Cultural background is an important element to take into account, as some countries are more accustomed than others to using, or are more willing to adopt, new smart technologies (Bouwman et al., 2010).

Furthermore, this study shows that education influences on attitude toward covert information collection. Future research could assess whether education influences users‘ tolerance of the privacy risk they are willing to take. Similarly, future research could replicate the model and analyse how the results vary according to age distribution.

Regarding the control variable gender, we decided to use a binary measure (male/female). However, societal norms on this are changing. Cartwright and Nancarrow (2022) suggested that, although at present the number of respondents who identify as belonging to the non-binary category is very low, it can be expected to increase as this identity becomes more accepted in society. Therefore, future research might leave the question open to respondents.

## REFERENCES


Aguirre, E., Roggeveen, A. L., Grewal, D., & Wetzels, M. (2016). The personalization-privacy paradox: Implications for new media. *Journal of Consumer Marketing*, *33*(2), 98-110.

Bajaj, A., & Nidumolu, S. R. (1998). A feedback model to understand information system usage. *Information and Management*, *33*(4), 213-224.

Bawack, R. E., Wamba, S. F., & Carillo, K. D. A. (2021). Exploring the role of personality, trust, and privacy in customer experience performance during voice shopping: Evidence from SEM and fuzzy set qualitative comparative analysis. *International Journal of Information Management*, *58*,102309.

Benlian, A., Klumpe, J., & Hinz, O. (2020). Mitigating the intrusive effects of smart home assistants by using anthropomorphic design features: A multimethod investigation. *Information Systems Journal*, *30*(6), 1010-1042.

Blut, M., Wang, C., Wünderlich, N. V., & Brock, C. (2021). Understanding anthropomorphism in service provision: a meta-analysis of physical robots, chatbots, and other AI. *Journal of the Academy of Marketing Science*, *49*(4), 632-658.

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, *48*(7), 953-977.

Bouwman, H., Carlsson, C., Castillo, F. J. M., Giaglis, G. M., & Walden, P. (2010). Factors affecting the present and future use of mobile data services: comparing the Dutch, Finnish and Greek markets. *International Journal of Mobile Communications*, *8*(4), 430-450.

Buhalis, D., & Moldavska, I. (2022). Voice assistants in hospitality: using artificial intelligence for customer service. *Journal of Hospitality and Tourism Technology*, *13*(3), 386-403.

Candao, G. C., Herrando, Carolina, H., & Martín-De, M. J. (2023), Affective Interaction with Technology: The Role of Virtual Assistants in Interactive Marketing, in Wang, C. (ed.). *The Palgrave Handbook of Interactive Marketing*, pp. 275-298

Carmines, E. G., & Zeller, R. A. (1979). Reliability and validity assessment. Sage publications.

Cartwright, T., & Nancarrow, C. (2022). A Question of Gender: Gender classification in international research. *International Journal of Market Research*, *64*(5), 575-593

Chen, Y.H., Keng, C.-J. & Chen, Y.-L. (2022), "How interaction experience enhances customer

engagement in smart speaker devices? The moderation of gendered voice and product smartness", *Journal of Research in Interactive Marketing*, *16*(3), pp. 403-419.

Epley, N., Waytz, A., & Cacioppo, J. T. (2007). On seeing human: a three-factor theory of anthropomorphism. *Psychological Review*, *114*(4), 864.

Foehr, J., & Germelmann, C. C. (2020). Alexa, can I trust you? Exploring consumer paths to trust in smart voice-interaction technologies. *Journal of the Association for Consumer Research*, *5*(2), 181-205.

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research, 8*(3), 382-388.

Foster, J. K., McLelland, M. A., & Wallace, L. K. (2022). Brand avatars: impact of social interaction on consumer–brand relationships. *Journal of Research in Interactive Marketing*, *16*(2), 237-258.

Frick, N. R., Wilms, K. L., Brachten, F., Hetjens, T., Stieglitz, S., & Ross, B. (2021). The perceived surveillance of conversations through smart devices. *Electronic Commerce Research and Applications*, *47*, 101046.

Gao, Y., & Liu, H. (2022). Artificial intelligence-enabled personalization in interactive marketing: a customer journey perspective. *Journal of Research in Interactive Marketing*, *17*(5), 1-18.

Geisser, S. (1974). A Predictive Approach to the Random Effects Model. *Biometrika*, *61*(1), 101-107

Go, E., & Sundar, S. S. (2019). Humanizing chatbots: The effects of visual, identity and conversational cues on humanness perceptions. *Computers in Human Behaviour*, *97*, 304-316.

Groom, V., Nass, C., Chen, T., Nielsen, A., Scarborough, J. K., & Robles, E. (2009). Evaluating the effects of behavioral realism in embodied agents. *International Journal of Human-Computer Studies*, *67*(10), 842-849.

Hair Jr, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European Business Review*, *28*(1), 63-76.

Han, S., & Yang, H. (2018). Understanding adoption of intelligent personal assistants: A parasocial relationship perspective. *Industrial Management and Data Systems*, *118*(3), 618-636.

Heerink, M., Kröse, B., Evers, V., & Wielinga, B. (2010). Assessing acceptance of assistive social agent technology by older adults: the almere model. *International Journal of Social Robotics*, *2*(4), 361-375.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1),115-135.

Ho, M. T., Mantello, P., Ghotbi, N., Nguyen, M. H., Nguyen, H. K. T., & Vuong, Q. H. (2022). Rethinking technological acceptance in the age of emotional AI: surveying Gen Z (Zoomer) attitudes toward non-conscious data collection. *Technology in Society*, *70*, 102011.

Hsieh, S. H., & Lee, C. T. (2021). Hey Alexa: examining the effect of perceived socialness in usage intentions of AI assistant-enabled smart speaker. *Journal of Research in Interactive Marketing*, *15*(2), 267-294.

Jung, Y., Choi, B., & Cho, W. (2021). Group satisfaction with group work under surveillance: The stimulus-organism-response (SOR) perspective. *Telematics and Informatics*, *58*, 101530.

Kang, H., & Kim, K. J. (2022). Does humanization or machinization make the IoT persuasive? The effects of source orientation and social presence. *Computers in Human Behavior*, *129*, 107152.

Ki, C. W. C., Cho, E., & Lee, J. E. (2020). Can an intelligent personal assistant (IPA) be your friend? Para-friendship development mechanism between IPAs and their users. *Computers in Human Behavior*, *111*, 106412.

Klumpe, J., Koch, O. F., & Benlian, A. (2020). How pull vs. push information delivery and social proof affect information disclosure in location based services. *Electronic Markets*, *30*(3), 569-586.

Kowalczuk, P. (2018). Consumer acceptance of smart speakers: a mixed methods approach. *Journal of Research in Interactive Marketing*, *12*(4), 418-431.

Krafft, M., Arden, C. M., & Verhoef, P. C. (2017). Permission marketing and privacy concerns—Why do customers (not) grant permissions? *Journal of Interactive Marketing*, *39*, 39-54.

Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on human-computer interaction*, *2*(CSCW), 1-31

Lavado-Nalvaiz, N., Lucia-Palacios, L., & Pérez-López, R. (2022). The Role of the Humanisation of Smart Home Speakers in the Personalisation–Privacy Paradox. *Electronic Commerce Research and Applications*, 53, 101146.

Lee, B. C. (2012). The determinants of consumer attitude toward service innovation–the evidence of ETC system in Taiwan. *Journal of Services Marketing*, *26*(1), 9-19.

Lee, J. M., & Rha, J. Y. (2016). Personalisation–privacy paradox and consumer conflict with the use of location-based mobile commerce. *Computers in Human Behaviour*, *63*, 453-462.

Lee, S. A., & Oh, H. (2021). Anthropomorphism and its implications for advertising hotel brands. *Journal of Business Research*, *129*, 455-464.

Libaque-Sáenz, C. F., Wong, S. F., Chang, Y., & Bravo, E. R. (2021). The effect of fair information practices and data collection methods on privacy-related behaviours: A study of mobile apps. *Information and Management*, *58*(1), 103284.

Lu, L., Cai, R., & Gursoy, D. (2019). Developing and validating a service robot integration willingness scale. *International Journal of Hospitality Management*, *80*, 36-51.

Lucia-Palacios, L., & Pérez-López, R. (2021). Effects of Home Voice Assistants' Autonomy on Instrusiveness and Usefulness: Direct, Indirect, and Moderating Effects of Interactivity. *Journal of Interactive Marketing*, *56*, 41-54.

Lucia-Palacios, L., & Pérez-López, R. (2023). How can autonomy improve consumer experience when interacting with smart products? *Journal of Research in Interactive Marketing*, *17*(1), 19-37.

Mathur, M. B., Reichling, D. B., Lunardini, F., Geminiani, A., Antonietti, A., Ruijten, P. A., & Szuts, A. (2020). Uncanny but not confusing: Multisite study of perceptual category confusion in the Uncanny Valley. *Computers in Human Behavior*, *103*, 21-30.

Melumad, S., & Meyer, R. (2020). Full disclosure: How smartphones enhance consumer self-disclosure. *Journal of Marketing*, *84*(3), 28-45.

Morey, T., Forbath, T., & Schoop, A. (2015). Customer data: Designing for transparency and trust. *Harvard Business Review*, *93*(5), 96-105.

Mori, M., (1970). The Uncanney Valley. *Energy* 7, (4), 33-35.

Nunnally, J. C. (1978). *Psychometric theory (2nd ed.)*. New York: McGraw-Hill.

Peltier, J. W., Dahl, A. J., & Schibrowsky, J. A. (2023). Artificial intelligence in interactive marketing: A conceptual framework and research agenda. *Journal of Research in Interactive Marketing (in press)*.

Pitardi, V., & Marriott, H. R. (2021). Alexa, she's not human but… Unveiling the drivers of consumers' trust in voice-based artificial intelligence. *Psychology and Marketing*, *38*(4), 626-642.

Plangger, K., & Montecchi, M. (2020). Thinking beyond privacy calculus: Investigating reactions to customer surveillance. *Journal of Interactive Marketing*, *50*, 32-44.

Poushneh, A. (2021). Humanizing voice assistant: The impact of voice assistant personality on consumers‘ attitudes and behaviors. *Journal of Retailing and Consumer Services*, *58*, 102283.

Reis, H. T., Maniaci, M. R., Caprariello, P. A., Eastwick, P. W., & Finkel, E. J. (2011). Familiarity does indeed promote attraction in live interaction. *Journal of Personality and Social Psychology*, *101*(3), 557.

Rhim, J., Kwak, M., Gong, Y., & Gweon, G. (2022). Application of humanization to survey chatbots: Change in chatbot perception, interaction experience, and survey data quality. *Computers in Human Behavior*, *126*, 107034.

Schaupp, L. C., & Carter, L. (2010). The impact of trust, risk and optimism bias on E-file adoption. *Information Systems Frontiers*, *12*(3), 299-309.

Siddike, M. A. K., Spohrer, J., Demirkan, H., & Kohda, Y. (2018). People‘s interactions with cognitive assistants for enhanced performances. 51st Hawaii International Conference on System Sciences, 10.24251/HICSS.2018.205

Song, M., Du, J., Xing, X., & Mou, J. (2022). Should the chatbot ‒save itself‖ or ―be helped by others‖? The influence of service recovery types on consumer perceptions of recovery satisfaction. *Electronic Commerce Research and Applications*, *55*, 101199.

Stone, M. (1974). Cross-validatory choice and assessment of statistical predictions. *Journal of the Royal Statistical Society: Series B (Methodological)*, *36*(2), 111-133.

Toader, D. C., Boca, G., Toader, R., Măcelaru, M., Toader, C., Ighian, D., & Rădulescu, A. T. (2019). The effect of social presence and chatbot errors on trust. *Sustainability*, *12*(1), 256.

Tsai, W. H. S., Liu, Y., & Chuan, C. H. (2021). How chatbots' social presence communication enhances consumer engagement: the mediating role of parasocial interaction and dialogue. *Journal of Research in Interactive Marketing*, *15*(3), 460-482.

Turow, J., Hennessy, M., & Draper, N. (2015). The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. *Available at SSRN 2820060*.

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547-559.

Waytz, A., Gray, K., Epley, N., & Wegner, D. M. (2010). Causes and consequences of mind perception. *Trends in Cognitive Sciences*, *14*(8), 383-388.

Xie, Y., Chen, K., & Guo, X. (2020). Online anthropomorphism and consumers‘ privacy concern: Moderating roles of need for interaction and social exclusion. *Journal of Retailing and Consumer Services*, *55*, 102-119.

Zlotowski, J. A., Sumioka, H., Nishio, S., Glas, D. F., Bartneck, C., & Ishiguro, H. (2015). Persistence of the uncanny valley: the influence of repeated interactions and a robot's attitude on its perception. *Frontiers in Psychology*, *6*, 883.

## APPENDIX 3

**Appendix 3.1.** Measures

| Latent variable | Items |
|---|---|
| Humanisation | HUM1: My smart home speaker has intentions.<br>HUM2: My smart home speaker has a mind of its own.<br>HUM3: My smart home speaker has consciousness.<br>HUM4: My smart home speaker has its own free will.<br>HUM5: My smart home speaker experiences emotions. |
| Social presence | SOCPRES1: When I interact with my smart home speaker I feel there is a sense of personalness.<br>SOCPRES2: When I interact with my smart home speaker I feel there is a sense of human contact.<br>SOCPRES3: When I interact with my smart home speaker I feel like if I am dealing with a real person.<br>SOCPRES4: When I interact with my smart home speaker I feel there is a sense of sociability.<br>SOCPRES5: When I interact with my smart home speaker I feel there is a sense of human sensitivity. |
| Perceived surveillance | SURV1: I personally believe I am being surveilled by my smart home speaker.<br>SURV2: I feel my behavior was being observed by my smart home speaker.<br>SURV3: I feel I am exposed to monitoring by my smart home speaker.<br>SURV4: While I‘m using my smart home speaker my behavior has to be kept under guard. |
| Trust | TRUST1: Smart speakers providers are trustworthy.<br>TRUST2: Smart speakers providers treat my personal information fairly and honestly.<br>TRUST3: I trust that smart speakers providers have my best interests in mind when dealing with my information.<br>TRUST4: I can trust the privacy policy of smart speakers providers. |
| Attitude toward covert information collection | COVERT1: I think using covert strategies like covert data collection is a good information collection system.<br>COVERT2: The fact that my smart home speaker collects data without my awareness / without my knowledge makes me feel good.<br>COVERT3: I prefer the speaker does not constantly request permission to collect data.<br>COVERT4: I like the idea that the smart home speaker is capturing information even though I am not actively using it. |

# CHAPTER IV

## NOTICE AND CHOICE AS TRUST-BUILDING MECHANISMS: THE IMPORTANCE OF INFORMATION TRANSPARENCY AND INFORMATION SENSITIVITY

## 4.1. INTRODUCTION

In the context of smart home speakers, the importance of privacy protection has been an important issue. Users have doubts about what information is collected, who is collecting it and what it is used for (Manikonda et al., 2018; Vilmalkumar et al., 2021). They demand control in terms of providing permission concerning whether to agree to data collection (Park et al., 2023) and an effective privacy policy that can reduce perceived privacy risks (Balapour, 2020) and increase trust (Bandara et al., 2020).

Trust is a central element in the use of digital services and smart home speakers characterised by privacy concerns and can encourage users to continue using these devices and recommend them to others (Widjaja et al., 2019; Wu et al., 2012). Previous research has examined how privacy policy statements can be used as trust-building mechanisms in the online environment (Wang and Herrando, 2019; Vila and Kuster, 2011; Wu et al., 2012). According to the privacy–trust–behavioural intention model (Liu et al., 2005), privacy policy statements reflect a firm‘s trustworthiness and honesty, as these statements increase the transparency of the information collection process (Slepchuk and Milne, 2020) and thus increase trust, which, in turn, influences consumer behaviour in an online context (e.g. repeat purchases, return visits and recommendations). Privacy policies are usually based on the US Federal Trade Commission (FTC) and include notice, choice, access and security as the main privacy protection practices. Of these, notice and choice require a more frequent active consumer response, so these two mechanisms are more visible than the others.

According to the FTC (1998), notice is the most important principle for privacy protection, as it is a transparency tool. Notice requires firms to inform users about their privacy policies regarding information collection, storing and sharing (Wu et al., 2012).

Choice offers users the option of consenting (or not consenting) to information collection, so it offers data control (Bornschein et al., 2020). This control can be managed once the user is given notice of the privacy policy (Obar and Oeldorf-Hirsch, 2020). Notice and choice are the variables that generate perceptions of power in users (Bornschein et al., 2020) and transparency (Liang et al., 2018). However, in terms of their relationship with trust development, results are mixed and scarce (Chang et al., 2018; Wu et al., 2012). For example, Chang et al. (2018) found that online notice influenced the perceived effectiveness of privacy policy (EPP), but they did not test the effect on trust. Wu et al. (2012) found that notice is related to user trust, but not choice. However, these studies do not examine the effects of notice and choice on consumer behaviour. Therefore, more research is needed to understand the impact of notice and choice on trust and consumer behaviour.

The effect of privacy policy – and thus notice and choice – on users‘ trust and behaviour will depend on user attitudes toward the collection, storage and use of personal information (Dinev et al., 2013; Rodríguez-Priego et al., 2023). How sensitive consumers are toward information collection and how important information transparency is for them are two relevant attitudinal traits that influence users‘ privacy risks (Dinev et al., 2013). In terms of information sensitivity, previous studies have mostly focused on its effects on perceived privacy risk and personal information disclosure (Hong et al., 2021; Ha et al., 2021; Chua et al., 2005; Bansal et al., 2016; Kehr et al., 2015; Bansal and Gefen 2010; Rohm and Milne, 2004; Kim et al., 2019; Mothersbaugh et al., 2012; Malhotra et al., 2004). The greater the degree of information sensitivity, the lower the utility of the benefits perceived for disclosing that information (Gouthier et al., 2022) and the greater the perceived privacy risks (Kim et al., 2019). Previous research has suggested that consumers should claim for greater control when

they perceive that the information collected is more sensitive (Rumboldand and Piercioknek, 2018; Chua et al., 2021). Thus, how much sensitive toward the information collected users are, may be relevant to explain to which extent they will value the possibility of choosing what information to share according to the company‘s privacy policy. However, to the authors‘ knowledge, there is no study that examines the role of information sensitivity in influencing the EPP and trust in a firm.

Although previous research has focused on firms‘ information transparency concerning privacy policies (Chung et al., 2022; Dehling and Sunyaev, 2023; Hung and Wong, 2009; Karwatzki et al., 2017; Walker, 2016), little is known about how users valuing information transparency can influence the EPP elements in building trust. In this case, the importance of information transparency is defined as ‗the consumer-rated importance of notifying the consumers what types of information a firm has collected about them, and how that information is going to be used‘ (Dinev et al., 2013, p. 303). The more important information transparency is in the online context, the greater the users‘ perceived risks and the lower their willingness to accept information collection or to take advantage of online personalised services (Awad and Krishnan, 2006). However, these studies did not address how the importance of information transparency can affect the role of notice actions in contributing to trust and the EPP.

This study has two objectives. First, it analyses whether notice and choice can improve EPP, user trust and intention to continue to use. Second, it examines the role played by users‘ information sensitivity (the degree thereof) and the importance of information transparency in the effects of notice and choice on EPP and trust. To achieve these goals, 679 users of smart home speakers were surveyed and their responses were analysed using structural equation modelling.

This research contributes to the literature on privacy in three ways. First, this study extends the literature about the role of notice and choice as trust-building mechanisms, showing that these two dimensions increase EPP, which, in turn, generates trust both directly and indirectly (Dinev et al., 2011; Mutimukwe et al., 2020; Chang et al., 2018). Further, our study shows that notice and choice can explain the intention to continue to use smart devices. Second, this study adds to previous research by showing that the extent to which notice and choice create trust when users interact with smart home speakers varies depending on individual information sensitivity and the importance assigned to information transparency. Both notice and choice are more important as trust-building mechanisms when users‘ information sensitivity is higher and for users that assign greater importance to information transparency. Third, the findings add to the debate on privacy by suggesting that the importance level of information transparency influences how notice affects EPP. In contrast to previous research, the present study examines the importance of information transparency as a moderating variable in the influence of notice on EPP and not as an antecedent of privacy risks (Dinev et al., 2013) or information disclosure (Awad and Krishnan, 2006).

## 4.2. LITERATURE REVIEW

### 4.2.1. Legal privacy framework

In 1970, the US Congress approved the *Privacy Protection Act*, which contained the main Fair Information Practice Principles (FIPPs). The FIPPs are composed of five dimensions: notification, choice, access, security and enforcement. A few decades later, in 1990, the Commission of the European Community published the European Union Data Protection Directive, which contained eight fundamental principles. Most of the

directives and norms implemented in Europe, Canada and the US focused on aspects such as notice and consent. These government regulations were followed by the FTC documents with suggestions on the implementation of privacy policies, and, in 2004, the Organisation for Economic Co-operation and Development outlined eight principles on _collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability‘ *(Recommendation of the Council of 23rd September 1980: Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data, Part Two, paragraphs 7–14).*

### 4.2.2. Privacy–trust–behavioural intention model

Privacy has been considered to play a critical role in the adoption and use of smart devices, including smart home speakers (Jasper and Pearson, 2022; Hong et al., 2020; Kowalzuc, 2019; Hsu and Lin, 2016). These devices collect privacy information that can be sensitive for users, as it is collected from a private environment (home) where different people co-live. With the growth of invasive digital technologies and algorithmic decision-making, consumers are more aware of privacy limits, and they demand more control and awareness about what type of information is collected, how it is collected and for what purpose; thus, they desire the right to deny information being collected in the first place (van Ooijen and Vrabec, 2019).

Based on the context of e-commerce and online interactions, the privacy–trust–behavioural intention model, proposed by Liu et al. (2005), suggests that an individual‘s perception of privacy significantly influences their trust in a platform or service. This trust, in turn, affects their behavioural intentions, such as willingness to engage in transactions or share personal information. The model acknowledges the critical role of privacy as a foundational element that underpins trust in digital interactions (Widjaja et al., 2019). Wu et al. (2012) adapted this model to study the effects of privacy policy on

trust and behaviour. When users feel confident that their privacy is protected and their data are handled securely, they are more likely to trust the service provider, which can lead to increase engagement and usage.

This model defines privacy policy using five dimensions: notice, choice, access, security and enforcement. Although these dimensions may improve user trust in online environments, findings about their effects are mixed, and not all of them have the same value for consumers (Wu et al., 2012). Although extant studies have used choice, access, security and enforcement to define privacy policy, only notice, access and security have been found to improve user trust. Chang et al. (2018) found that online notice influences EPP but did not test its relationship with trust. In the context of institutional trust, Wang and Herrando (2019) found that institutional privacy assurance, related to the EPP, increases trust in social commerce, social interaction and, hence, users‘ purchase intention and actual purchase behaviour. Bornschein et al. (2020) employed choice and visibility (notice) and showed that these variables help create a position of power in users and, at the same time, reduce the risk they perceive when disclosing private information.

Under regulations such as the General Data Protection Regulation in the European Union, explicit consent is required for certain types of data-processing activities. Among the variables that define and explain the above-mentioned privacy policies, notice and choice are the most visible to the user and are intended to provide a foundation for user autonomy and control over personal data. Both are signals companies send to consumers and that require active action on the user side (Chang et al., 2018; Gluck et al., 2016; Liu et al., 2022). Regarding notice, the company provides the user with information about its privacy policy, and, in many cases, users must explicitly accept it. Notice refers to the disclosure and explanation of the privacy policy

regarding the information collected (Wu et al., 2012). It informs users about what data are being collected, how the data are being used, who the data are shared with and the purposes of these activities. The goal is to ensure that users are fully informed about the privacy implications of their interactions with a service or product. Consumers are obligated to read the privacy policy and confirm that they have been informed.

Choice refers to giving customers the option to select what collected personal information can be used and how and by who it will be used (Bornschein et al., 2020). Users should be provided with options to opt in or out of certain data collection practices. In the case of choice, consumers must proactively take action to determine the extent to which they want to protect their privacy, thus empowering users. Companies can reduce consumers‘ privacy concerns by ensuring they are aware of information collection strategies and giving them the choice to agree to said collection and to eliminate or remove their personal data (Rhom and Milne, 2004). Table 4.1 shows a literature review about the effect of notice and choice on consumer behaviour, from which it is evident that there is no consensus on how privacy policy tools influence user behaviour. Although some research has shown that they provide control and build trusting relationships with the company (Chang et al., 2018; Hooper and Vos, 2009; Rodríguez-Priego et al., 2023; Schoenbachler and Gordon, 2002; Xu et al., 2008), other studies question this (Brough et al., 2022; Liu, 2014). Additionally, not all studies analyse the same elements within privacy policies, and some studies have shown that not all elements of privacy policies have the same impact on users (Wu, 2012).

**Table 4.1.** Literature on trust-building strategies

| Authors | Context | Variables | Main findings |
|---|---|---|---|
| Benson et al. (2015) | Social network sites | Privacy notice and control | When the users of social network sites perceive the sites to provide security notices, they are more likely to trust the site and voluntarily share their information. The users consider security notices to be important attributes of an online service and feel more comfortable dealing with a provider that offers an approval notice or informs users of the implications of such notices. |
| Bornschein et al. (2020) | Websites | Choice/visibility | Choice and visibility help create a position of power in users and, at the same time, reduce the perceived risk when disclosing private information. |
| Brough et al. (2022) | Publicly traded companies | Cookie notice | Protective privacy notices often have the unintended consequence of reducing consumer trust and interest in making a purchase. |
| Chang et al. (2018) | Online banking websites | EPP, notice and choice | Being informed about the information collected makes users more aware that the information is not incorrect or incomplete, thus improving EPP. Notice, access, security and enforcement have a positive effect on EPP. EPP helps to improve perceived control and reduce privacy risks, which, in turn, improves user trust. |
| Culnan and Armstrong (1999) | Interactive home information services | EPP | An effective policy based on explicitly communicating to users that fair information practices are respected can increase trust. Customers will be more willing to continue the relationship with the company, allowing the company to benefit from the collection and use of data resulting from that relationship. |
| Dehling and Sunyaev (2023) | Information systems | Privacy policy transparency | The theory of transparency of information privacy practices (TIPP) is developed. It is shown that privacy notices are not a useful transparency artifact and that better artifact designs are necessary to establish TIPP. Designs must be more flexible and tailored to consumers to achieve lasting alignment between suppliers and users. |
| Flavian and Guinaliu (2006) | Websites | Perception of security with regard to the handling of personal data | The greater consumers‘ perception of security with regard to the handling of their personal data, the greater their trust in a website. |
| Guo et al. (2022) | Websites | Transparency, notice and protection | Transparency, control and protection as privacy policy elements positively influence EPP. Additionally, privacy policy transparency has almost no effect on the benevolence of privacy-conscious users. |
| Hooper and Vos (2009) | Websites | Privacy notice | The privacy notice is the primary means of informing users about a company‘s privacy policy and represents a commitment between the user and the company receiving the information. |

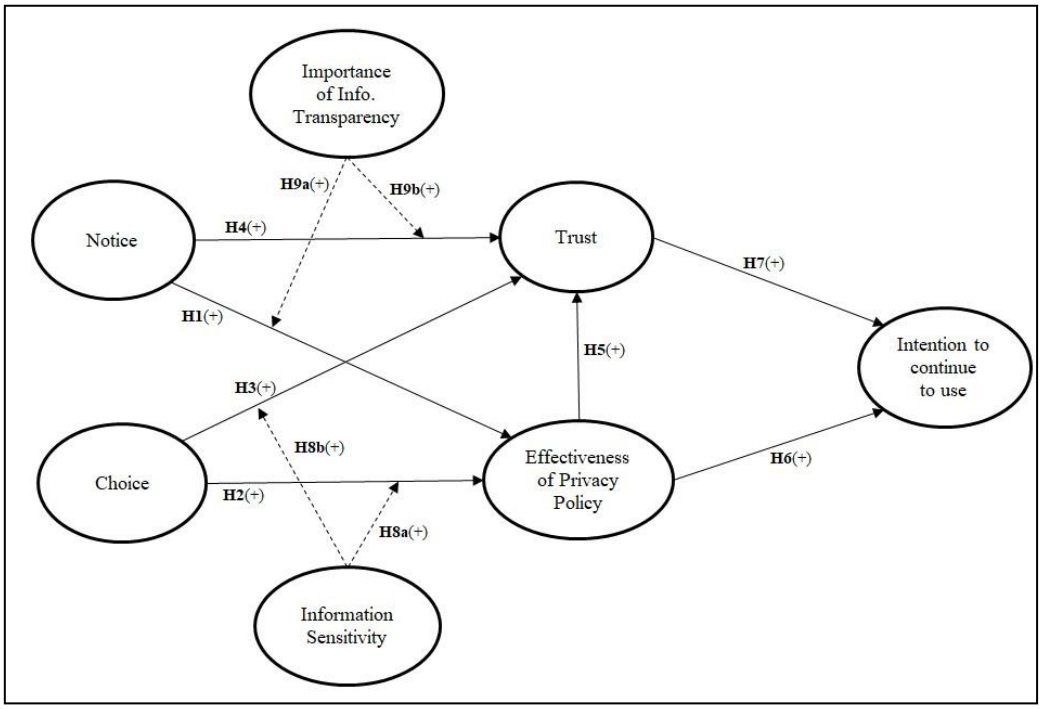
**Table 4.1 (continued).** Literature on trust-building strategies

| Authors | Context | Variables | Main findings |
|---|---|---|---|
| Liu (2014) | Mobile app | Notice and consent | In the context of mobile commerce, the notice and consent measure is not very helpful in improving control. Offering users meaningful alternatives to data collection, encouraging better monitoring and control by third parties and providing more effective and user-friendly warnings and alerts are proposed to improve users‘ control over their information. |
| Liu et al. (2022) | App | Privacy feedback and choice | When companies inform users about their data practices, users perceive the service provider as being more trustworthy. |
| Milne and Culnan (2004) | Internet | Notice and EPP | It is found that reading is associated with privacy concerns, positive perceptions of understanding the notice and higher levels of trust in the notice. This suggests that effective privacy notices have an important role to play in addressing the risks associated with e-commerce. |
| Mutimukwe et al. (2020) | E-services | EPP | EPP influences individual trust beliefs, nondisclosure behaviour and perceptions of privacy control for all services. |
| Obar and Oeldorf-Hirsch (2020) | Networking site | Privacy policy notice | It is proposed that, if the user has notice of the privacy policy, they will have more control over the data. They suggest that the notice and choice model of privacy protection does not provide the results needed to ensure privacy protection. |
| Rodríguez-Priego et al. (2023) | Online customer care | Perceived customer care/perceived control | Sending clear signals to users giving them notice and asking for explicit permission about the information collected creates a sense of control and power. |
| Rohm and Milne (2004) | Personal medical information | Choice | Consumers express a high degree of concern and a low level of trust in the organisations that collect, use and share their personal health data. Giving users the choice to agree to information collection or to remove personal data can reduce consumers‘ privacy concerns. |
| Schoenbachler and Gordon (2002) | Postal service | Credibility | Clear and reliable privacy policy helps companies to improve their reputation, thereby strengthening the ties between the user and the company. |
| Wang and Herrando (2019) | E-commerce sites | EPP | Institutional privacy assurance, which is related to EPP, increases trust in social commerce. |
| Wu et al. (2012) | Websites | Notice/choice | Under the privacy–trust–behavioural intention model, it is shown that, of the elements comprising a privacy policy (notice, choice, access, security and enforcement), only notice, access and security serve as trust-building mechanisms in the online environment. |
| Xu et al. (2008) | Websites | EPP | An effective privacy policy increasers users‘ feelings of control. EPP has a significant impact on reducing privacy risks. |

## 4.3. HYPOTHESIS DEVELOPMENT

This section proposes a theoretical model based on the privacy–trust–behavioural intention model to address the thesis‘s goals in the context of smart home speakers. This study proposes that notice and choice, as important dimensions of privacy policy, can impact EPP and trust, and these, in turn, will affect the intention to continue to use the smart home speaker. Trust is defined as the degree to which an organisation can be trusted to protect users‘ personal information (Bawack et al., 2021; Chang et al., 2018). Therefore, trust plays a key role in increasing consumer confidence to share their personal information when using smart home speakers (Pitardi and Marriott, 2021). Further, this study proposes that users‘ information sensitivity and the importance of information transparency can moderate the effects of notice and choice on EPP and trust. Figure 4.1 shows the proposed model.

**Figure 4.1**. Theoretical model



### 4.3.1. The effects of notice and choice on EPP, trust and behaviour

Sending clear signals to users, giving them notice and asking for explicit permission about the information to be collected can provide them with a sense of control and power (Bornschein et al., 2020; Rodríguez-Priego et al., 2023). This perception of control reduces the asymmetry between the company and the user, as the latter is more aware of how information is collected and handled. Notice refers to the extent to which consumers are informed about the collection and use of their data (Malhotra et al., 2004). Being notified makes users more aware that the information collected is not incorrect or incomplete, which provides them with more security and control over their information (Wu et al., 2012), thereby improving EPP (Chang et al., 2018). Although some studies have found that the mere presence of a notice statement is enough to increase users‘ perceived control (Arcand et al., 2007), others have highlighted that users must read the notice and the opt in for information collection (Milne and Culnan, 2004). In other words, it is necessary for users to choose whether they share their personal information. In both cases, when users perceive that they have power over their personal information, they tend to expect positive outcomes from the handling of their personal information (Brandimarte et al., 2013). Individuals who can choose what personal information they wish the company to use may come to perceive that the privacy policy is effective (Balapour et al., 2020; Chang et al., 2018). Therefore, we propose the following:

**H1.** *Notice will have a positive effect on EPP.*

**H2.** *Choice will have a positive effect on EPP.*

Companies have different methods of building a trustworthy relationship with consumers, one of which is providing a privacy policy. Notice is the main way of

informing users about the privacy policy of a company and represents a commitment between users and the company receiving the information (Hooper and Vos, 2009). Giving users a choice is perceived as a sign of honesty and respect for users‘ privacy. In addition, if the company informs users about data practices, users perceive the service provider as trustworthy (Liu et al., 2022). Previous research has shown that, when consumers feel that they have control over their information, they tend to have a higher level of trust toward disclosing personal information to third parties (Rodríguez-Priego et al., 2023). Choice defaults have been found to be an important tool in providing consumers with control over their personal information (Veltri and Ivchenko, 2017). Given that notice and choice create a greater sense of control for users (Bornschein et al., 2020) and that perceived control reinforces trust (Aïmeur et al., 2016; Taddei and Contena, 2013), we propose the following:

**H3.** *Choice will have a positive effect on trust.*

**H4.** *Notice will have a positive effect on trust.*

### 4.3.2. The consequences of Effectiveness of Privacy Policy

Some studies have argued that, to build trust, privacy policies should be clear, informative and reassure consumers that the risk of disclosing private information is very low (Dinev and Hart, 2006; Wu et al., 2012). A clear and reliable privacy policy helps companies to improve their reputation, thereby strengthening the relationship between users and the company (Schoenbachler and Gordon, 2002). Thus, an effective privacy policy increases trust (Mutimukwe et al., 2020; van Slyke et al., 2006; Culnan and Armstrong, 1999). Therefore, we propose the following:

**H5.** *EPP will have a positive effect on trust.*

Security and privacy are key factors that can help predict customer satisfaction with a service provider (Liu et al., 2008). Service providers that decrease users‘ privacy concerns increase their satisfaction (Liang et al., 2014). As argued above, a robust and effective privacy policy will increase users‘ perceived privacy protection and, at the same time, reduce their privacy concerns (Chang et al., 2018; Xu et al., 2008). Likewise, a company that displays its privacy policies and seeks to make them more effective creates an image of caring about its consumers, which ensures users will continue using the service. Thus, we propose the following:

**H6.** *EPP will have a positive effect on intention to continue to use.*

As trust increases, individuals‘ expectations that organisations will respect their right to decide how their information will be used also increase. Trust is a key attribute for consumers to trade with a company, especially when the transaction occurs using a machine only, without interacting with a human being (Gefen and Straub, 2004). In the context of voice assistants, previous research has established a positive relationship between trust and intention to continue to use (Pitardi and Marriot, 2021; Yang et al., 2015; Gao et al., 2015), and this Thesis has already confirmed this relationship. Previous empirical studies have suggested that a high level of trust in service providers results in continued purchase and use, whereas a lack of trust leads to the opposite outcome (Gao et al., 2015; Yang et al., 2015; Zhou, 2013). Therefore, we propose the following:

**H7.** *Trust will have a positive effect on intention to continue to use.*

### 4.3.3. Moderating variables: information sensitivity and the importance of information transparency

Smart home speakers use and require a large amount of information to provide a personalised service. This information can be demographic, financial, behavioural or about personal preferences. It can be collected by the device directly but also through other applications or devices connected to the smart home speaker (Benlian et al., 2019; Frick et al., 2021). When interacting with these devices, users are aware of the information they are providing, especially if they are asked for consent or are warned that the information will be collected. Concerns may vary depending on the type of information collected or the degree of information sensitivity of each user (Peterson et al., 2007). Typically, the major concerns for users are the strategies used by the device to collect the information and how the service provider uses their data (Kim et al., 2019).

When users are asked for more sensitive information, they become more aware that they are disclosing information and become concerned about their privacy (Ha et al., 2021). Similarly, Xu et al. (2009) have argued that, when users are asked for permission in mobile applications, they become aware of the possible information collection and focus their attention on whether to give permission. Typically, users are reluctant to provide sensitive information, and, when they are asked to, they become more aware of the importance of a strong privacy policy (Balapour et al., 2020; Petersen et al., 2007).

Despite the importance of information sensitivity in privacy research, previous studies have mostly focused on its effect on the use of mobile apps, especially banking apps, and on information disclosure (Kim et al., 2019; Mothersbaugh et al., 2012). However, to the authors‘ knowledge, there is no study that examines the impact of this

variable on the relationship between choice and users‘ perceived trust. It has been demonstrated that, when consumers have several choice options, they generally prefer and choose the default option (van Ooijen and Vraken, 2019). Providing consent by changing a default setting (i.e. opting in) requires the individual to engage in a conscious and affirmative action and, hence, exerts a form of control. Users that are more sensitive toward personal information collection may perceive this control as more important. Therefore, consumers that perceive that personal information collection is sensitive value the opportunity to choose whether to collect that information. Accordingly, a privacy policy will create more trust in users and will be perceived as more effective.

**H8a.** *Information sensitivity will have a positive moderating effect on the relationship between choice and EPP.*

**H8b**. *Information sensitivity will have a positive moderating effect on the relationship between choice and trust.*

*Importance of information transparency*

Due to the advance of new technologies and smart devices, consumers are increasingly demanding transparency from companies concerning how much information is collected about them, when it is collected, for what purpose it is collected and how it is going to be used (Bandara et al., 2020). Smart home speakers that have a microphone and sensors to collect data pose a further risk to consumers‘ privacy. In this research, the importance of information transparency is defined as the consumer-rated importance of being notified about what types of information a firm has collected about them, as well as how and for what purpose it will be used (Dinev et al., 2013; Stone et al., 1983; Awad and Krishnan, 2006). This construct was proposed by Awad and

Krishnan (2006), who based it on the utility maximisation theory and suggested that consumers who value information transparency features are less willing to be profiled for personalised offerings. A similar result was found between consumers‘ disposition to value privacy and willingness to be profiled online (Karwatzki et al., 2017). This result confirms what Awad and Krishnan (2006) suggested: consumers that have a disposition to value information transparency will have a higher disposition to value privacy, which, in turn, influences their assessment of privacy risks. To the best of our knowledge, the usefulness of privacy policy statements with respect to individuals‘ disposition to value information transparency and trust has not been examined.

Following similar constructs as disposition to privacy outlined by Li (2004), disposition to information transparency represents a general attitude toward information transparency. This disposition is the desire of transparency about the use of personal information and suggests that people have different levels of transparency expectations and assign different levels of importance to transparency.

Informing the consumer about the collection and use of personal data indicates that the firm cares about consumers‘ privacy by demonstrating transparency and benevolence, which, in turn, increases trust (Venkatesh et al., 2016). Previous research has found that consumers with low privacy concerns do not care about privacy policies (Guo et al., 2022). Therefore, for consumers with high privacy concerns and, therefore, a disposition to value information transparency, privacy policy tools will have a stronger impact on the EPP of firms. Similarly, consumers with a high disposition to value information transparency will value information collection notices more than consumers with a low disposition, which, in turn, will generate higher levels of trust.

**H9a:** *Importance of information transparency will have a positive moderating effect on the relationship between notice and EPP.*

**H9b:** *Importance of information transparency will have a positive moderating effect on the relationship between notice and trust.*

## 4.4. METHODOLOGY

To test these hypotheses, the same data as previous chapters has been used. From the initial 700 responses, only 679 users of smart home speakers were included in the sample. The age of participants ranged between 18 and 70, and there was a mix of men and women. Most of the respondents owned Alexa, followed by Google Assistant and then HomePod. The frequency of use of smart home speakers is very high. Table 4.2 details the sample demographics that have been discussed in previous chapters.

**Table 4.2.** Sample characteristics

| **Gender (%)** | | **Education (%)** | | **Frequency (%)** | | **Brand (%)** | | **Income $ (%)** | | **Age (%)** | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| F | 55.52 | N | 1.03 | N | 0.44 | Alexa | 65.87 | < 20,000 | 5.30 | 18–24 | 3.09 |
| M | 44.48 | C | 7.36 | AN | 1.62 | Cortana | 1.07 | 20,000–39,999 | 11.93 | 25–34 | 56.55 |
| | | B | 61.86 | S | 17.38 | Google | 23.27 | 40,000–59,999 | 24.45 | 35–44 | 23.71 |
| | | M/PHD | 29.75 | AED | 50.66 | HomePod | 9.79 | 60,000–79,999 | 22.39 | 45–54 | 10.75 |
| | | | | ED | 29.99 | | | 80,000–99,999 | 23.56 | 55–64 | 4.27 |
| | | | | | | | | > 100,000 | 12.08 | > 65 | 1.62 |
| | | | | | | | | No disclosure | 0.29 | | |

***Note**: F: female; M: male; N: none; C: college; B: bachelor; M/PHD: Master/PhD; N: never; AN: almost never; S: sometimes; AED: almost every day; ED: every day.*

The variables were measured using constructs tested by previous research. All the constructs were reflected and measured on a seven-point Likert scale, where 1 = ‗completely disagree' and 7 = ‗completely agree'. The final dependent variable, continue to use, was based on three items adapted from Bhattacharjee (2001) and Han and Yang (2018). The variable trust was based on four items outlined by Lee and Rha

(2016). EPP was based on three items outlined by Xu et al. (2008). Notice and choice were both based on three items from Wu et al. (2012) and Chang et al. (2018). The two moderating variables were also reflective. Information sensitivity was based on five items adapted from Kim et al. (2019) and disposition to information sensitivity was based on four items from Awad and Krishnan (2006), see Appendix 4.1 (Appendix 4).

Control variables were added to the study. Age was an open-ended response, education was a categorical variable formed by four levels, gender was a dummy variable (male = 1 and female = 0) and use frequency was a categorical variable formed by five levels.

## 4.5. RESULTS

### 4.5.1. Common method bias

The existence of a common method bias was controlled for and this was achieved in two ways: procedural control and statistical control. In terms of statistical control, apart from the Harman‘s single-factor method, two additional tests were carried out to control for common method bias. Following Kock and Lynn (2012), the model was run using a new _random‘ variable (a single-indicator latent variable) to obtain the variance inflation factor (VIF) values of all model variables. The results show that the VIF values are equal to or lower than 3.3, so the model can be considered free of common method bias (see Table 4.3). According to the results of Harman‘s single-factor method, a single factor explained 17.9% of the variance, whereas the whole model explained the variance up to 74.6%. In terms of procedural control, common method bias is related to the survey or questionnaire design (MacKenzie and Podsakoff, 2012). Following MacKenzie and Podsakoff (2012), to avoid this type of bias, the

researchers pointed out to the respondents that all responses were anonymous and that there were no correct answers. Additionally, we randomly ordered the questions and items in the survey to hide the researchers‘ interest and conceal the relationship between dependent and independent variables. This ensured the two variable types were psychologically separated (Podsakoff et al., 2012).

### 4.5.2. Measurement model validation

Exploratory analysis was carried out to test the unidimensionality of the constructs. To do this, SPSS software was used, followed by SmartPLS software to conduct confirmatory analysis. In doing so, the existence of seven constructs was confirmed. Then, the internal consistency of the measurement model was analysed (see Table 4.3). As can be seen, Cronbach‘s alpha values and the composite reliability index exceeded the minimum acceptable value of 0.7 (Bagozzi and Yi, 1988; Nunnally, 1978). The average variance extracted (AVE) values were above 0.5 for all latent variables, exceeding the threshold of 0.6 (Hair et al., 2014) and confirming convergent validity. Regarding discriminant validity, the heterotrait–monotrait (HTMT) ratios were below 0.85 (Henseler et al., 2015), confirming the discriminant validity of the model (see Table 4.4). Correlations between variables were also below the AVE square roots (Fornell and Larcker, 1981), further confirming the discriminant validity.

**Table 4.3.** Items and measurement model

| | VIF | Loadings | Cronbach's alpha | Composite reliability | AVE | Mean | Standard deviation |
|---|---|---|---|---|---|---|---|
| **Notice** | 2.16 | | 0.853 | 0.911 | 0.773 | 4.931 | 1.399 |
| NOT_1 | | 0.904 | | | | | |
| NOT_2 | | 0.886 | | | | | |
| NOT_3 | | 0.910 | | | | | |
| **Choice** | 2.14 | | 0.883 | 0.931 | 0.810 | 4.836 | 1.387 |
| CH_1 | | 0.863 | | | | | |
| CH_2 | | 0.886 | | | | | |
| CH_3 | | 0.888 | | | | | |

**Table 4.3. (Continued).** Items and measurement model

| | VIF | Loadings | Cronbach's alpha | Composite reliability | AVE | Mean | Standard deviation |
|---|---|---|---|---|---|---|---|
| **EPP** | 1.71 | | 0.856 | 0.912 | 0.776 | 5.071 | 1.246 |
| EPP_1 | | 0.878 | | | | | |
| EPP_2 | | 0.868 | | | | | |
| EPP_3 | | 0.896 | | | | | |
| **Trust** | 1.24 | | 0.902 | 0.931 | 0.773 | 4.961 | 1.151 |
| TRUST_1 | | 0.888 | | | | | |
| TRUST_2 | | 0.879 | | | | | |
| TRUST_3 | | 0.888 | | | | | |
| TRUST_4 | | 0.861 | | | | | |
| **Continue to use** | 1.10 | | 0.773 | 0.868 | 0.688 | 5.371 | 0.832 |
| CONT_1 | | 0.864 | | | | | |
| CONT_2 | | 0.741 | | | | | |
| CONT_3 | | 0.874 | | | | | |
| **Information sensitivity** | 1.21 | | 0.871 | 0.906 | 0.660 | 5.271 | 1.221 |
| IS_1 | | 0.828 | | | | | |
| IS_2 | | 0.839 | | | | | |
| IS_3 | | 0.754 | | | | | |
| IS_4 | | 0.830 | | | | | |
| IS_5 | | 0.807 | | | | | |
| **Information transparency** | 1.26 | | 0.828 | 0.885 | 0.658 | 5.32 | 0.900 |
| TRANS_1 | | 0.819 | | | | | |
| TRANS_2 | | 0.813 | | | | | |
| TRANS_3 | | 0.840 | | | | | |
| TRANS_4 | | 0.772 | | | | | |

**Table 4.4.** Discriminant validity

| | CONT | TRUST | NOTICE | CHOICE | EPP | IS | TRANS |
|---|---|---|---|---|---|---|---|
| **CONT** | **0.830** | *0.179* | *0.250* | *0.286* | *0.360* | *0.413* | *0.442* |
| **TRUST** | 0.156 | **0.879** | *0.395* | *0.369* | *0.444* | *0.224* | *0.179* |
| **NOTICE** | 0.209 | 0.354 | **0.900** | *0.851* | *0.753* | *0.753* | *0.369* |
| **CHOICE** | 0.232 | 0.324 | 0.756 | **0.879** | *0.696* | *0.288* | *0.295* |
| **EPP** | 0.298 | 0.392 | 0.656 | 0.595 | **0.881** | *0.315* | *0.444* |
| **IS** | 0.343 | 0.203 | 0.317 | 0.343 | 0.279 | **0.812** | *0.785* |
| **TRANS** | 0.353 | 0.161 | 0.319 | 0.353 | 0.378 | 0.667 | **0.811** |

***Note**: Values (in bold) on the diagonal are the AVE square roots. Values below the diagonal are correlations between variables. Values above the diagonal are the HTMT ratio values. CONT: continue to use; EPP: perceived effectiveness of privacy policy; IS: information sensitivity; TRANS: information transparency.*

### 4.5.3. Structural results

Table 4.5 shows the structural results. Four models were developed. Model 1 only includes the direct effects of the variables, model 2 includes the moderating effect of information sensitivity, model 3 includes the moderating effect of the importance of information transparency and model 4 includes both moderating effects. The results are very similar for all models, showing great consistency.

To test the predictive relevance, SmartPLS 4.0 software (www.smartpls.de) was used, which provides the $Q^2$ value recommended by Stone (1974) and Geisser (1974). The four models show positive $Q^2$ values for the main dependent variables.

The results show that notice and choice have a positive and significant effect on EPP, so H1 and H2 are supported. Notice has a significant direct effect on trust, meaning that H4 is supported, but choice does not have a significant effect, meaning that H3 is not supported. EPP has a positive effect on trust and intention to continue to use, but, unexpectedly, trust has no significant effect on intention to continue to use. Therefore, H5 and H6 are supported, but H7 is not.

**Table 4.5.** Structural results

| **Variables** | **Model 1** | **Model 2** | **Model 3** | **Model 4** |
|---|---|---|---|---|
| Choice → EPP | 0.231*** | 0.234*** | 0.212*** | 0.222*** |
| Notice → EPP | 0.481*** | 0.441*** | 0.404*** | 0.407*** |
| Choice → Trust | 0.071 | 0.077 | 0.064 | 0.063 |
| Notice → Trust | 0.124** | 0.103* | 0.116** | 0.098* |
| EPP → Trust | 0.269*** | 0.243** | 0.247** | 0.251** |
| EPP → Continue | 0.266*** | 0.266*** | 0.266** | 0.266** |
| Trust → Continue | 0.043 | 0.043 | 0.043 | 0.043 |
| **Moderating effects** | **Model 1** | **Model 2** | **Model 3** | **Model 4** |
| Information Sensitivity → EPP | | 0.121*** | | -0.027 |
| Information Sensitivity → Trust | | 0.104** | | 0.147*** |
| Information Sensitivity × Choice → EPP | | 0.090** | | 0.057* |
| Information Sensitivity × Choice → Trust | | 0.046** | | 0.022 |

**Table 4.5. (Continued)** Structural results

| **Moderating effects** | **Model 1** | **Model 2** | **Model 3** | **Model 4** |
|---|---|---|---|---|
| Transparency → EPP | | | 0.236** | 0.248*** |
| Transparency → Trust | | | 0.046 | -0.046 |
| Transparency × Notice → EPP | | | 0.088** | 0.058* |
| Transparency × Notice → Trust | | | 0.070** | 0.063** |
| **Control variables** | **Model 1** | **Model 2** | **Model 3** | **Model 4** |
| Age → Continue | 0.034 | 0.034 | 0.034 | 0.034 |
| Gender → Continue | -0.005 | -0.005 | -0.005 | -0.005 |
| Education → Continue | -0.083** | -0.083** | -0.083** | -0.083** |
| Freq → Continue | 0.089** | 0.089** | 0.089** | 0.089** |
| $R^2/Q^2$ EPP | 0.453/0.444 | 0.475/0.456 | 0.498/0.477 | 0.505/0.477 |
| $R^2/Q^2$ Trust | 0.172/0.124 | 0.182/0.135 | 0.180/0.133 | 0.191/0.135 |
| $R^2/Q^2$ Continue | 0.105/0.057 | 0.105/0.059 | 0.105/0.086 | 0.105/0.075 |

***Note**: ***significant at 1%; **significant at 5%; *significant at 10%.*

As the effect of choice on trust was unexpected, the mediating effects were analysed using the Preacher–Hayes method. According to the results, EPP mediates the relationship between notice and trust, as well as choice and trust (Table 4.6). When the model has no direct effect of EPP on trust, the effect of choice on trust is 0.1332 (t = 2.43, p = 0.015). Therefore, EPP exerts a total mediating effect between choice and trust. Related to notice, EPP exerts a partial mediating effect between notice and trust.

**Table 4.6.** Analysis of mediation effects notice and choice on trust

| **Total effect on trust** | | **Direct and indirect effects on trust** | | | |
|---|---|---|---|---|---|
| | **Coefficient** | **Direct effect** | **Mediators** | **Indirect effect** | **95% CI** |
| Notice | 0.2531*** | 0.1238** | EPP | 0.1293 | (0.068;0.200) |
| Choice | 0.1332** | 0.0710 | EPP | 0.0621 | (0.022; 0.110) |

***Note**: ***significant at 1%; **significant at 5%; *significant at 10%; 95% CI: 95% confidence interval.*

According to the privacy–trust–behavioural intention model, the effects of privacy perceptions on behaviour take place through trust; however, we are interested in knowing whether both notice and choice have indirect effects on intention to continue to use, as well as the extent to which trust mediates these relationships. Thus, the direct

effect of choice and notice on intention to continue to use was included in the model. The results show that choice and notice have indirect effects on intention to continue to use mediated by EPP but not by trust in the service provider (Table 4.7). Further, choice has a positive and direct effect on intention to continue to use[2].

**Table 4.7.** Analysis of mediation effects of notice and choice on intention to continue to use

| **Total effect on continue to use** | | **Direct and indirect effects on continue to use** | | | |
|---|---|---|---|---|---|
| | **Coefficient** | **Direct effect** | **Mediators** | **Coefficient** | **95% CI** |
| Notice | 0.1933*** | 0.0240 | **EPP** | **0.1570** | **(0.070; 0.23)** |
| | | | Trust | 0.0061 | (-0.008; 0.020) |
| | | | EPP–Trust | 0.0062 | (-0.008; 0.020) |
| | | | *Total effect* | 0.1690 | (0.080; 0.250) |
| Choice | 0.2205*** | 0.0906** | **EPP** | **0.1205** | **(0.050; 0.120)** |
| | | | Trust | 0.0044 | (-0.080;0.020) |
| | | | EPP–Trust | 0.0049 | (-0.080; 0.020) |
| | | | *Total effect* | 0.1299 | (0.060; 0.200) |

***Note**: ***significant at 1%; **significant at 5%; *significant at 10%; 95% CI: 95% confidence interval.*

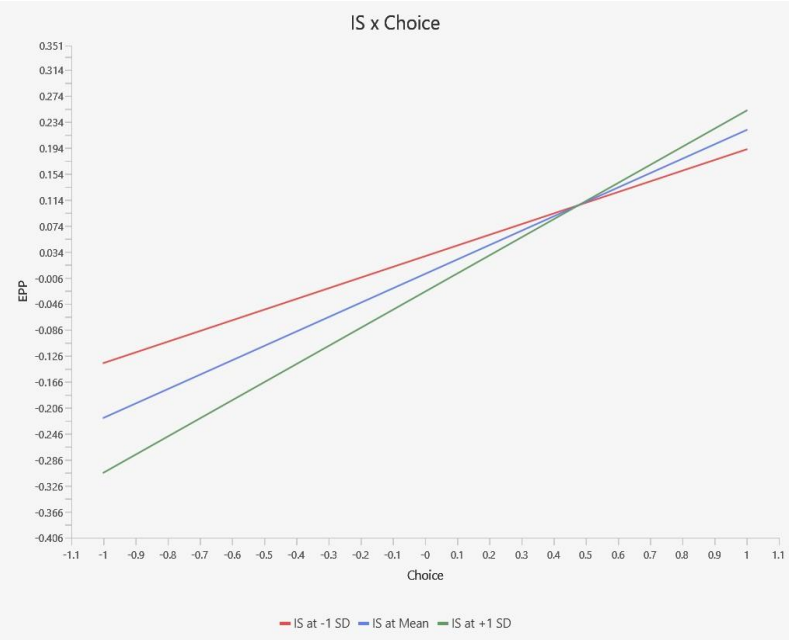
In terms of moderating effects, mixed results were found. Information sensitivity positively moderates the effect of choice on EPP, thereby supporting H8a (see Figure 4.2). Additionally, information sensitivity positively moderates the effect of choice on trust, and this moderation is significant in model 2 but not in model 4, where it shows less robustness. Related to information transparency, it positively moderates the effects of notice on both EPP and trust, supporting H9a and H9b (see Figures 4.3 and 4.4).

The results show that the effect of choice on EPP is stronger for those with high sensitivity to personal information collection by the smart home speaker. For high values of perceptions about choice (users who perceive that the smart home speaker gives them the possibility to choose what information to share very clearly), the effect

[2] Table 4.7 shows the results provided by the Preacher–Hayes method, but the four models shown in Table 4.5 were also run in SmartPLS, including the effects of choice and notice on intention to continue to use. The results were almost the same with no variation in the sign or level of significance of the already found effects. The $R^2$ of the whole model was 0.111. See the Appendix 4.2. for the models estimated in SmartPLS.

of this variable on EPP is higher for those with high information sensitivity (Figure 4.2). In contrast, for low perceptions of choice possibilities, the effects on EPP are higher for users with low information sensitivity.

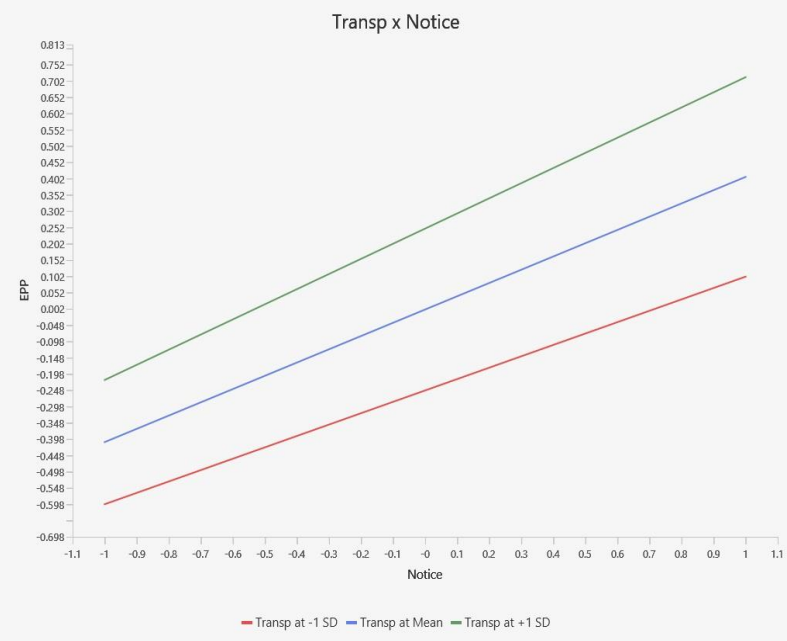
**Figure 4.2.** Moderating effect of information sensitivity on the relationship between choice and EPP




*IS: information sensitivity; EPP: perceived effectiveness of privacy policy.*

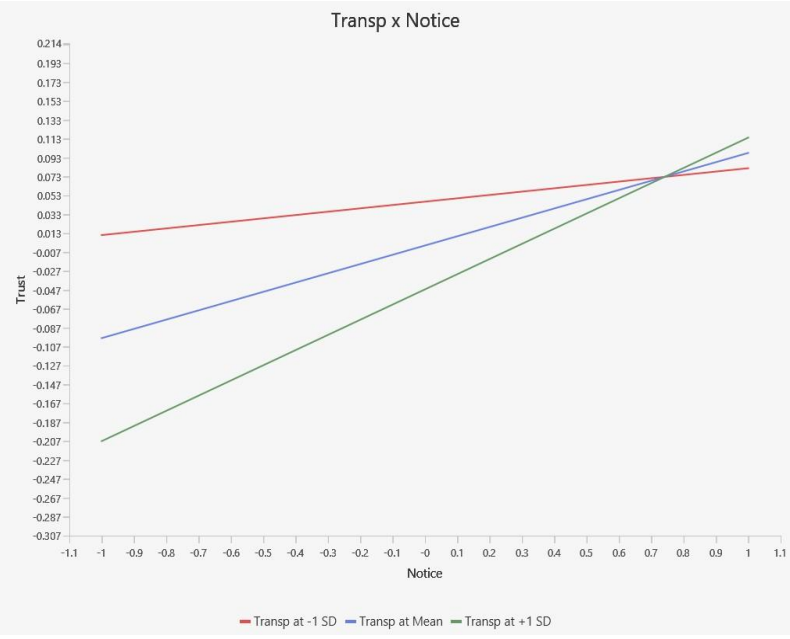
The results show that the effects of notice on both EPP and trust are stronger for consumers who give more importance to information transparency. The value of EPP due to notice is higher for users who value more information transparency regardless of the level of notice perceptions (Figure 4.3). This difference is slightly greater for higher levels of notice. In the case of trust, low levels of notice generate less trust for high importance levels of information transparency (Figure 4.4). For high levels of perceived notice, the difference between the two groups of users is reduced.

**Figure 4.3.** Moderating effect of the importance of information transparency on the relationship between notice and EPP




*EPP: perceived effectiveness of privacy policy; Transp: importance of information transparency*

**Figure 4.4.** Moderating effect of the importance of information transparency on the relationship between notice and trust




*Transp: importance of information transparency*

To better understand the results, the moderating effect of EPP when choice has an indirect effect on trust was examined. For this purpose, the Preacher-Hayes method was applied. The index of moderated mediation is 0.0294 bootstrap 95% CI = (0.009;

0.0548). Therefore, the indirect effect of choice on trust mediated by EPP is more positive for higher levels of personal information collection sensitivity.

Related to control variables, frequent users have a greater intention to continue using smart home speakers, whereas users with a higher education level are more reluctant to continue using them. Neither gender nor age are relevant in explaining the intention to continue using smart home speakers.

## 4.6. DISCUSSION

This study had two aims. The first was to understand the effects of notice and choice as trust-building mechanisms in the context of smart home speakers and how they influence the intention to continue using them. The second was to examine the moderating effect of information sensitivity and user importance of information transparency on the role of notice and choice as trust-building mechanisms.

The findings support the positive effect of notice and choice on EPP, confirming previous research (Balapour et al., 2020; Chang et al., 2018). Additionally, this research confirms the privacy–trust–behavioural intention model proposed by Liu (2005). The findings suggest that notice has a direct and indirect effect on trust mediated by the EPP, whereas choice has an indirect effect on trust completely mediated by EPP. These results are consistent with extant studies that highlight the positive effect of notice and choice (Bornschein et al., 2020; Dinev et al., 2013). However, they contradict the results of other studies, which suggest that only notice influences EPP (Chang et al., 2018) and trust (Wu et al., 2012). This study confirms that, when users feel they have the control over their data (the information collection process is disclosed or overt, and users have

the choice to deny the information being collected), EPP is more likely to be higher, which generates trust for the service provider.

An interesting result is the effect of notice and choice on intention to continue to use. Although previous research has examined the direct effect of notice and choice on trust (Wu et al., 2012), this study provides new evidence of how notice and choice influence intention to continue to use. This study finds an indirect effect of both variables on intention to continue to use through EPP and a direct effect of choice on intention to continue to use. This direct effect complements the predictions made by the privacy–trust–behavioural intention model. This finding is consistent with previous research on customer satisfaction, which suggests that, when users can decide what information they want to disclose and are able to configure their privacy policy, they have a more positive experience, are more satisfied, and reward this with positive behaviour (Cheng et al., 2023) such as greater intentions to continue to use.

Privacy policies can be valued differently depending on user characteristics and privacy concerns (Guo et al., 2022; Bansal et al., 2015). This research suggests that users‘ sensitivity toward information collection and the importance of information transparency are two vital variables that should be considered. Consumers who are more sensitive to sharing personal information will probably have more privacy concerns and will value their own privacy to a greater extent. Similarly, consumers who value information transparency will probably show higher levels of privacy concerns. This result is consistent with the findings of Guo et al. (2022), who examined the moderating effect of privacy concerns on the relationship between transparency, control and protection (as privacy dimensions) and vulnerability and benevolence. The results add the positive moderating effect of information sensitivity and information transparency on the effect of notice and choice on EPP and trust.

## 4.7. CONCLUSION

### 4.7.1. Theoretical contributions

This study contributes to previous research in three ways. First, it contributes to the privacy–trust–behavioural intention model proposed by Liu et al. (2005). Research on privacy policies has mainly addressed the context of websites and apps (Bornschein et al., 2020; Chang et al., 2018; Liu et al., 2022; Obar and Oeldorf-Hirsch, 2020); however, little is known about the effect of privacy policy elements in the context of voice assistants. As previous research has not reached a consensus about the effect of privacy policy elements on trust, this study contributes with new evidence about this issue by examining not only direct effects but also indirect effects. This results show that only notice has a direct effect on trust, whereas choice influences trust through EPP. Further, not only are notice and choice trust-building mechanisms, but they also promote the intention to continue to use smart home speakers. This research suggests that choice and notice increase intention to continue to use in a different way. Whereas choice has a direct impact on intention to continue to use intention, notice only has an indirect effect by increasing EPP. The findings contribute by showing the important role of EPP in the generation of trust and in improving intention to continue to use. Therefore, these privacy policy elements have an impact on consumer‘s behaviour. This is very relevant, as firms are concerned with increasing the use of these products by consumers to create a habit.

Second, this study contributes to privacy research by providing new evidence of how the effect of privacy policy on consumer behaviour is dependent on individuals‘ attitudes toward information privacy. It examines how two personal dispositions may influence the role of notice and choice as trust-building mechanisms: information sensitivity and the importance of information transparency. Although information

sensitivity has been examined as an antecedent of privacy concern or as a moderator in studies of willingness to disclose personal information (Aiello et al., 2020; Bansal and Gefen, 2010; Kang et al., 2022; Mothersbaough et al., 2012; Rohm and Milne, 2004; Sun et al., 2022; Tao et al., 2024), little is known about how it can influence the impact of privacy policies on consumers‘ behaviour. The study contributes with new findings that reveal the effectiveness of choice as a trust-building mechanism, suggesting that is greater when users perceive that the collection of personal information by the smart home speaker is sensitive.

Third, this study contributes to information privacy research by examining the moderating effect of the importance of information transparency on the relationships between notice and EPP, as well as between notice and trust (Awad and Krishnan, 2006; Dinev et al., 2013). Although previous research has mainly examined consumers‘ perceptions of firm transparency (Aiello et al., 2020; Chung et al., 2022; Kim et al., 2019; Sansome et al., 2024), little is known about how the value that consumers give to information transparency influence privacy policies as trust-building mechanisms. Awad and Kishnan (2006) showed that the importance of information transparency may diminish the users‘ willingness to be profiled online for personalised services; they also showed that it mediates the relationship between privacy concerns and privacy policy importance on this willingness. Further, Dinev et al. (2013) showed that this attitudinal variable increased perceived risks in Web 2.0 services. These results extend this research by showing that the importance of information transparency can also act as moderator in the relationships between notice and EPP and between notice and trust.

### 4.7.2. Implications for managers

This study is timely and needed in the context of smart technologies, which have raised the issue of information privacy to the forefront of contemporary societal issues, a priority line of research for the Marketing Science Institute. The results offer insights that are useful for managers.

These findings suggest that companies should implement notice and choice statements in their privacy policies, as they can increase EPP and, hence, trust and the intention to continue to use smart home speakers. In fact, these two dimensions are key determinants of EPP. Nevertheless, though notice has direct effects on both EPP and trust, choice influences trust indirectly through EPP. Therefore, companies should especially focus on improving the design of privacy policy content, especially in terms of notification, to respond to consumers‘ growing concerns in this area. They should ensure these notices are simple, accessible, appealing and clear for all types of users to understand.

Overall, the participants in the sample provided good values for both notice and choice statements in the survey (means are close to five over seven), but some users provided low levels of perceived notice and choice. Firms should consider that low levels of perceived notice and choice will decrease trust in firms. Thus, ensuring a high assessment of notice and choice options is important. According to the results, companies should detect the type of users of their devices in terms of valuing information sensitivity and information transparency, as these characteristics influence how much consumers value notice and choice. Companies should ensure clarity in their choice options, especially for individuals that are more sensitive to sharing personal information. Further, notifications should be especially clear and well designed for

those that value information transparency. To determine user type, companies should conduct questionnaires for users about information collection sensitivity and how much they value information transparency when they start using smart home speakers.

### 4.7.3. Limitations and future research lines

This research is not without limitations. First, this study focused on notice and choice because both are signals that the company sends to users and require active action on their side. However, other privacy policy tools could be included in future research that can provide new evidence of the role played by privacy policies in influencing consumers‘ behaviour. Second, though the current research has focused on intention to continue to use the smart home speaker as a consumers‘ behavioural response, future research could examine the effects of privacy policy tools on other cognitive responses such as satisfaction or recommendation, as well as on emotional responses such as fatigue or stress. Further, it would be interesting to examine the usefulness of firms‘ privacy policy elements to reduce negative perceptions in the use of these devices, such as perceived surveillance. Third, the methodology used in this research was survey based, and experimental studies with different situations or privacy tools may offer more evidence and further the understanding of consumer behaviour and privacy concerns. Finally, this study is cross-sectional, and it may be interesting to examine the long-term evolution of the influence of privacy policies in this context. Future research could test the influence of user experiences with these devices on privacy concerns by comparing the perceptions of new users and more experienced users.

## REFERENCES


Akdeniz, B., Calantone, R. J., & Voorhees, C. M. (2013). Effectiveness of marketing cues on consumer perceptions of quality: The moderating roles of brand reputation and third-party information. *Psychology and Marketing, 30*(1), 76–89

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management, 52*, 102063.

Bartel Sheehan, K. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing, 13*(4), 24-38.

Benlian, A., Klumpe, J., & Hinz, O. (2019). Mitigating the intrusive effects of smart home assistants by using anthropomorphic design features: A multimethod investigation. *Information Systems Journal, 30*(6), 1010-1042.

Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social media users: does control over personal information, user awareness and security notices matter?. *Information Technology & People, 28*(3), 426-441.

Bornschein, R., Schmidt, L., & Maier, E. (2020). The effect of consumers‘ perceived power and risk in digital information privacy: The example of cookie notices. *Journal of Public Policy & Marketing, 39*(2), 135-154.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science, 4*(3), 340-347.

Brough, A. R., Norton, D. A., Sciarappa, S. L., & John, L. K. (2022). The bulletproof glass effect: Unintended consequences of privacy notices. *Journal of Marketing Research, 59*(4), 739-754.

Brill, T. M., Munoz, L., & Miller, R. J. (2022). Siri, Alexa, and other digital assistants: a study of customer satisfaction with artificial intelligence applications. In *The Role of Smart Technologies in Decision Making* (pp. 35-70). Routledge.

Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers‘ perceived privacy. *Government Information Quarterly, 35*(3), 445-459.

Chen, S. J., Tran, K. T., Xia, Z. R., Waseem, D., Zhang, J. A., & Potdar, B. (2023). The double-edged effects of data privacy practices on customer responses. *International Journal of Information Management, 69*, 102600.

Child, J. T., & Petronio, S. (2011). Unpacking the paradoxes of privacy in CMC relationships: The challenges of blogging and relational communication on the internet. *Computer-Mediated Communication in Personal Relationships*, 21-40.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104-115.

De Bellis, E., & Johar, G. V. (2020). Autonomous shopping systems: Identifying and overcoming barriers to consumer adoption. *Journal of Retailing*, *96*(1), 74-87.

Dehling, T., & Sunyaev, A. (2023). A design theory for transparency of information privacy practices. *Information Systems Research*, *8*(8), 1-22.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61-80.

Eagly, A. H., & Wood, W. (1999). The origins of sex differences in human behavior: Evolved dispositions versus social roles. *American Psychologist*, *54*(6), 408.

Eagly, A. H., & Wood, W. (2013). The nature–nurture debates: 25 years of challenges in understanding the psychology of gender. *Perspectives on Psychological Science*, *8*(3), 340-357.

Erdem, T., & Swait, J. (1998). Brand Equity as a Signaling Phenomenon. *Journal of Consumer Psychology*, 7(2), 131–157

Erdem, T., & Swait, J. (2004). Brand credibility, brand consideration, and choice. *Journal of Consumer Research*, *31*(1), 191-198.

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. *Industrial Management & Data Systems*, *106*(5), 601-620.

Foehr, J., & Germelmann, C. C. (2020). Alexa, can I trust you? Exploring consumer paths to trust in smart voice-interaction technologies. *Journal of the Association for Consumer Research*, *5*(2), 181-205-

Francis, B., Hasan, I., Park, J. C., & Wu, Q. (2015). Gender differences in financial reporting decision making: Evidence from accounting conservatism. *Contemporary Accounting Research*, *32*(3), 1285-1318.

Frener, R., & Trepte, S. (2022). Theorizing gender in online privacy research. *Journal of Media Psychology, 34(2),* 77-88.

Frick, N. R., Wilms, K. L., Brachten, F., Hetjens, T., Stieglitz, S., & Ross, B. (2021). The perceived surveillance of conversations through smart devices. *Electronic Commerce Research and Applications*, 101046.

Ganesan, S. (1994). Determinants of long-term orientation in buyer-seller relationships. *Journal of Marketing*, *58*(2), 1-19.

Gefen, D., & Straub, D. W. (2004). Consumer trust in B2C e-Commerce and the importance of social presence: experiments in e-Products and e-Services. *Omega*, *32*(6), 407-424.

Gluck, J., Schaub, F., Friedman, A., Habib, H., Sadeh, N., Cranor, L. F., & Agarwal, Y. (2016). How short is too short? Implications of length and framing on the effectiveness of privacy notices. *Twelfth Symposium on Usable Privacy and Security*, 321-340.

Greenwood, S., Perrin, A., & Duggan, M. (2016). Social media update 2016. *Pew Research Center*, *11*(2), 1-18.

Guo, Y., Wang, X., & Wang, C. (2022). Impact of privacy policy content on perceived effectiveness of privacy policy: the role of vulnerability, benevolence and privacy concern. *Journal of Enterprise Information Management*, *35*(3), 774-795.

Ha, Q. A., Chen, J. V., Uy, H. U., & Capistrano, E. P. (2021). Exploring the privacy concerns in using intelligent virtual assistants under perspectives of information sensitivity and anthropomorphism. *International Journal of Human–Computer Interaction*, *37*(6), 512-527.

Hooper, T., & Vos, M. (2009). Establishing business integrity in an online environment: An examination of New Zealand web site privacy notices. *Online Information Review*, *33*(2), 343-361.

Islas-Cota, E., Gutierrez-Garcia, J. O., Acosta, C. O., & Rodríguez, L. F. (2022). A systematic review of intelligent assistants. *Future Generation Computer Systems*, *128*, 45-62.

Jain, S., Basu, S., Dwivedi, Y. K., & Kaur, S. (2022). Interactive voice assistants–Does brand credibility assuage privacy risks?. *Journal of Business Research*, *139*, 701-717.

Kanwal, M., Burki, U., Ali, R., & Dahlstrom, R. (2022). Systematic review of gender differences and similarities in online consumers‘ shopping behavior. *Journal of Consumer Marketing*, *39*(1), 29-43.

Kim, D. J. (2012). An investigation of the effect of online consumer trust on expectation, satisfaction, and post-expectation. *Information Systems and e-Business Management*, *10*, 219-240.

Kim, D., Park, K., Park, Y., & Ahn, J. H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, *92*, 273-281.

Kowalczuk, P. (2018). Consumer acceptance of smart speakers: a mixed methods approach. *Journal of Research in Interactive Marketing*, *12*(4), 418-431.

Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on human-computer interaction*, *2*(CSCW), 1-31.

Lin, X., & Wang, X. (2020). Examining gender differences in people‘s information-sharing decisions on social networking sites. *International Journal of Information Management*, *50*, 45-56.

Liu, B., Miltgen, C. L., & Xia, H. (2022). Disclosure decisions and the moderating effects of privacy feedback and choice. *Decision Support Systems*, *155*, 113717.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S. (2005). Beyond concern a privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, *42*(2), 289-304.

Liu, X., He, M., Gao, F., & Xie, P. (2008). An empirical study of online shopping customer satisfaction in China: a holistic perspective. *International Journal of Retail & Distribution Management*, *36*(11), 919-940.

Liu, Y. (2014). User control of personal information concerning mobile-app: Notice and consent?. *Computer Law & Security Review*, *30*(5), 521-529.

Liu, B., Miltgen, C. L., & Xia, H. (2022). Disclosure decisions and the moderating effects of privacy feedback and choice. *Decision Support Systems*, *155*, 113717.

MacDonald, K. (1995). Evolution, the five-factor model, and levels of personality. *Journal of P ersonality*, *63*(3), 525-567.

Manikonda, L., Deotale, A., & Kambhampati, S. (2018, December). What's up with privacy? User preferences and privacy concerns in intelligent personal assistants. In *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*, 229-235.

Mari, A., & Algesheimer, R. (2021). The role of trusting beliefs in voice assistants during voice shopping. In Proceedings of the 54th Hawaii International Conference on System Sciences, 4073-4082.

Maroufkhani, P., Asadi, S., Ghobakhloo, M., Jannesari, M. T., & Ismail, W. K. W. (2022). How do interactive voice assistants build brands' loyalty? *Technological Forecasting and Social Change*, *183*, 121870.

Mazurek, G., & Małagocka, K. (2019). Perception of privacy and data protection in the context of the development of artificial intelligence. *Journal of Management Analytics*, *6*(4), 344-364.

McCole, P., Ramsey, E., & Williams, J. (2010). Trust considerations on attitudes toward online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research*, *63*(9-10), 1018-1024.

McGill, T., & Thompson, N. (2021). Exploring potential gender differences in information security and privacy. *Information & Computer Security*, *29*(5), 850-865.

McLean, G., & Osei-Frimpong, K. (2019). Hey Alexa… examine the variables influencing the use of artificial intelligent in-home voice assistants. *Computers in Human Behavior*, *99*, 28-37.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*(3), 15-29.

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing*, *58*(3), 20-38.

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of Service Research*, *15*(1), 76-98.

Mutimukwe, C., Kolkowska, E., & Grönlund, Å. (2020). Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Government Information Quarterly*, *37*(1), 101413.

Murphy, G. B., & Tocher, N. (2011). Gender differences in the effectiveness of online trust building information cues: An empirical examination. *The Journal of High Technology Management Research*, *22*(1), 26-35.

Namin, A. (2017). Revisiting customers' perception of service quality in fast food restaurants. *Journal of Retailing and Consumer Services*, *34*, 70-81.

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128-147.

Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly*, 115-143.

Petronio, S. (2002). Boundaries of privacy. Albany: State University of New York.

Petronio, S., & Gaff, C. (2010). Managing privacy ownership and disclosure. *Family communication about genetics: Theory and practice*, 120-135.

Rodríguez-Priego, N., Porcu, L., Pena, M. B. P., & Almendros, E. C. (2023). Perceived customer care and privacy protection behavior: The mediating role of trust in self-disclosure. *Journal of Retailing and Consumer Services*, *72*, 103284.

Rohm, A. J., & Milne, G. R. (2004). Just what the doctor ordered: The role of information sensitivity and trust in reducing medical information privacy concern. *Journal of Business Research*, *57*(9), 1000-1011.

Santouridis, I., & Veraki, A. (2017). Customer relationship management and customer satisfaction: the mediating role of relationship quality. *Total Quality Management & Business Excellence*, *28*(9-10), 1122-1133.

Schmitt, D. P., Realo, A., Voracek, M., & Allik, J. (2008). Why can't a man be more like a woman? Sex differences in Big Five personality traits across 55 cultures. *Journal of Personality and Social Psychology*, *94*(1), 168.

Schoenbachler, D. D., & Gordon, G. L. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. *Journal of Interactive Marketing*, *16*(3), 2-16.

Sun, Y., Wang, N., Shen, X. L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*, *52*, 278-292.

Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior*, *93*, 1-12.

Veltri, G. A., & Ivchenko, A. (2017). The impact of different forms of cognitive scarcity on online privacy disclosure. *Computers in Human Behavior*, *73*, 238-246.

Vila, N., & Kuster, I. (2011). Consumer feelings and behaviours towards well designed websites. *Information & Management*, *48*(4-5), 166-177.

Vimalkumar, M., Sharma, S. K., Singh, J. B., & Dwivedi, Y. K. (2021). _Okay google, what about my privacy?‘: User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior*, *120*, 106763.

Wang, Y., & Herrando, C. (2019). Does privacy assurance on social commerce sites matter to millennials?. *International Journal of Information Management*, *44*, 164-177.

Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, *28*(3), 889-897.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View. *ICIS 2008 Proceedings*. 6.

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2012). Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information Systems Research*, *23*(4), 1342-1363.

Yang, Q., Gong, X., Zhang, K. Z., Liu, H., & Lee, M. K. (2020). Self-disclosure in mobile payment applications: Common and differential effects of personal and proxy control enhancing mechanisms. *International Journal of Information Management*, *52*, 102065.

Yeh, J. C., Hsiao, K. L., & Yang, W. N. (2012). A study of purchasing behavior in Taiwan's online auction websites: Effects of uncertainty and gender differences. *Internet Research*, *22*(1), 98-115.

Zhang, J., Li, H., (Robert) Luo, X., & Warkentin, M. (2017). Exploring the Effects of the Privacy-Handling Management Styles of Social Networking Sites on User Satisfaction: A Conflict Management Perspective. Decision Sciences, 48(5), 956-989.

## APPENDIX 4

**Appendix 4.1.** Measures

| Latent variable | Items |
|---|---|
| Notice | NOT1: My smart home speaker discloses what personal information is going to be collected<br>NOT2: My smart home speaker explains why personal information is going to be collected<br>NOT3: My smart home speaker explains how the collected personal information will be used |
| Choice | CH1: My smart home speaker informs me whether my personal information will be disclosed to a third party and explains under what conditions it will be disclosed.<br>CH2: My smart home speaker gives clear choice (asking permission) before disclosing personal information to third party.<br>CH3: My smart home speaker gives clear choice (asking permission) before it uses my personal information for secondary purposes. |
| Effectiveness of privacy policy | EPP1: I feel confident that my smart home speaker provider privacy statements reflect their commitments to protect my personal information.<br>EPP2: With their privacy statements, I believe that my personal information will be kept private and confidential by the provider of my smart home speaker.<br>EPP3: I believe that my smart home speaker provider privacy statements are an effective way to demonstrate their commitments to Privacy. |
| Importance of Information Transparency | TRANSP1: I think it is important to know if my smart home speaker provider is going to use the information it collects from me in a way that identifies me.<br>TRANSP2: I think it is important to know how long my smart home speaker provider will keep the information it collects about me in its database.<br>TRANSP3: I think it is important to know what information my smart home speaker provider keeps about me in their databases.<br>TRANSP4: I think is important to know why and for what purpose, the smart home speaker is collecting information from me. |
| Information Sensitivity | IS1: The fact that my smart home speaker collects personal (demographic) information is very sensitive to me.<br>IS2: The fact that my smart home speaker collects physical information is very sensitive to me.<br>IS3: The fact that my smart home speaker collects financial information is very sensitive to me.<br>IS4: The fact that my smart home speaker collects activity information is very sensitive to me.<br>IS5: The fact that my smart home speaker collects information from other devices is very sensitive to me. |
| Trust | TRUST1: Smart speakers providers are trustworthy.<br>TRUST2: Smart speakers providers treat my personal information fairly and honestly.<br>TRUST3: I trust that smart speakers providers have my best interests in mind when dealing with my information.<br>TRUST4: I can trust the privacy policy of smart speakers providers. |
| Intention to continue to use | CONT1: I will frequently use the smart home speaker in the future.<br>CONT2: I intend to continue using the smart home speaker rather than discontinue its use.<br>CONT3: I will use the smart home speaker on a regular basis in the future. |

**Appendix 4.2.** Structural results: Direct relationship with intention to continue to use

| **Variables** | **Model 1** | **Model 2** | **Model 3** | **Model 4** |
|---|---|---|---|---|
| Choice → EPP | 0.232*** | 0.234*** | 0.212*** | 0.222*** |
| Notice → EPP | 0.481*** | 0.441*** | 0.405*** | 0.407*** |
| Choice → Trust | 0.071 | 0.103 | 0.064 | 0.063 |
| Notice → Trust | 0.124* | 0.077 | 0.116* | 0.098* |
| EPP →Trust | 0.269*** | 0.243*** | 0.247*** | 0.251*** |
| EPP → Continue | 0.223*** | 0.230** | 0.230*** | 0.230*** |
| Trust → Continue | 0.036 | 0.036 | 0.036 | 0.036 |
| **Notice → Continue** | **-0.052** | **-0.052** | **-0.052** | **-0.052** |
| **Choice → Continue** | **0.121*** | **0.121*** | **0.121*** | **0.121*** |
| **Moderating effects** | | | | |
| Information Sensitivity → EPP | | 0.121** | | -0.027 |
| Information Sensitivity → Trust | | 0.104** | | 0.147** |
| Information Sensitivity x Choice → EPP | | 0.090** | | 0.057* |
| Information Sensitivity x Choice → Trust | | 0.046* | | 0.022 |
| Transparency → EPP | | | 0.236*** | 0.248*** |
| Transparency → Trust | | | 0.046 | -0.046 |
| Transparency x Notice → EPP | | | 0.0885** | 0.058* |
| Transparency x Notice → Trust | | | 0.070** | 0.063** |
| **Control variables** | | | | |
| Age → Continue | 0.037 | 0.037 | 0.037 | 0.037 |
| Gender → Continue | -0.008 | -0.008 | -0.008 | -0.008 |
| Education → Continue | -0.089** | -0.089** | -0.089** | -0.089** |
| Freq → Continue | 0.091** | 0.091** | 0.091** | 0.091** |
| $R^2$/ $Q^2$ EPP | 0.453/0.444 | 0.476/0.456 | 0.498/0.477 | 0.505/0.477 |
| $R^2$/ $Q^2$ Trust | 0.172/0.124 | 0.182/0.135 | 0.180/0.133 | 0.191/0.135 |
| $R^2$/ $Q^2$ Continue | 0.111/0.054 | 0.111/0.056 | 0.111/0.079 | 0.111/0.070 |

***Note**: ***significant at 1%; **significant at 5%; *significant at 10%*

# CHAPTER V

## GENERAL DISCUSSION AND CONCLUSIONS

The use of smart devices such as Google Home, Amazon‘s Alexa or Apple‘s HomePod has changed how individuals perform many daily activities (including content consumption, interacting with companies, buying products, and switching on the heating). This technology facilitates a continuous exchange of information between users and companies. User information is constantly collected to return a bespoke user experience tailored to individual tastes and preferences (Go and Sundar, 2019; Gahler et al., 2023). Information collection has, though, brought information privacy to the forefront of consumers‘ worries and societal policy-making. This makes it an important topic for both academics and practitioners.

From a business perspective, effectively managing these concerns will enable companies to build closer ties with consumers and break down pertinent barriers. Users‘ privacy concerns and perceptions can also directly impact companies‘ income (vis-à-vis fewer purchases and greater litigation costs) (Bandara et al., 2020).

Academically, the Marketing Science Institute has stated that privacy concerns in the context of AI-enabled devices are a research priority from 2022 to 2024. In the context of smart products, privacy is a key user concern and one of the main barriers holding back these devices‘ adoption and use. Much research has focused on the role of privacy concerns and risks during smart home speaker adoptions. There is, however, less literature on post-adoption behaviours (e.g., the intention to continue use).

This thesis takes a post-use perspective toward smart home speakers. We have attempted to broaden the existing understanding of both smart home speaker use and user behaviour. The findings shed light on people‘s willingness to use these devices once they are aware of the benefits and disadvantages regarding privacy. This thesis has attempted to expand existing knowledge about (a) consumers‘ attitudes toward how

their personal information is collected when using smart home speakers and (b) the technology‘s antecedents and consequences.

The relationships between humanisation, surveillance, social presence, trust, and attitudes toward covert data collection practices have not been analysed in depth. Although privacy policies might reduce privacy concerns arising from smart home speaker use, few scholars have focused on how effective these policies are at fostering trust. Prior research has also not examined (a) the role of users‘ attitudes toward how their data is managed and (b) the link between privacy policy and trust formation.

It was proposed to study how companies can create trust, reduce the negative consequences of privacy loss due to data collection, and hence boost user intentions to continue using their smart home speakers. We engaged in three interrelated empirical studies to pursue this primary objective.

*Study 1 (Chapter II)*

The first study aimed to analyse how personalised smart home speaker communication influences user attitudes toward data collection (distinguishing between overt and covert collection practices). This study also focused on whether personalised communication through trust and attitudes toward (overt and covert) personal data collection can influence the intention to continue to use.

To achieve these objectives, privacy calculus theory and the personalisation-privacy paradox were used. The goal was to explore (a) whether the value of receiving personalised information can determine attitudes toward (overt and covert) information collection practices and (b) whether it can build trustworthy relationships between users and service providers. In doing so, a post-use perspective toward smart home speakers

was adopted. This perspective allowed us to gain first-hand insight into users‘ real-life experiences with smart home speakers.

The findings suggest that the value of message personalisation improves user attitudes toward both types of information collection (overt and covert). A positive relationship between personalisation value and trust and between trust and intention to continue to use was found. The findings demonstrate trust‘s important role in information management and the mediating role it plays between perceived personalisation value and the intention to continue to use.

*Study 2 (Chapter III)*

The second study examined how smart home speaker humanisation can both improve user attitudes toward covert information collection and build trust. It is also studied how smart home speaker humanisation can reduce surveillance perceptions.

To approach these objectives, this study developed a theoretical framework built on the humanisation literature and parasocial relationship theory. It is explored how smart home speaker characteristics can impact both user trust in service providers and attitudes toward covert data collection.

The results reveal that humanisation helps increase feelings of social presence and improves user attitudes toward covert data collection. This study also showed that low humanisation levels have a negative influence on trust; when humanisation increases, trust increases. Humanisation also has a negative impact on perceived surveillance. It was also found that user attitudes toward data collection are positive if users trust the service provider (even when users know that their data is being covertly collected).

*Study 3 (Chapter IV)*

The third study aimed to uncover whether notice and choice can (a) improve the perceived effectiveness of privacy policies and trust and (b) enhance the intention to continue to use. It also analysed the roles of information sensitivity and the importance of information transparency in notice‘s and choice‘s impact on the effectiveness of privacy policies and trust.

This study relied on the privacy-trust-behavioural intention model to achieve these objectives. This study explored whether notice and choice signal an effective privacy policy for building user trust. The chapter also analysed whether consumers with positive attitudes toward information transparency value the notice of information collection, which in turn generates higher levels of trust. It then examined whether choice messages are important in trust-building for consumers who are more sensitive about their personal information collection.

The findings show that notice has both direct and indirect effects on trust (as mediated by privacy policy effectiveness). That said, choice only has a total indirect effect on trust mediated by privacy policy effectiveness. The study results suggest that users are more likely to perceive a company‘s privacy policy as effective and trust the service provider when they feel in control of their data. The findings also show that notice and choice influence the intention to continue to use. While choice has a direct effect on the intention to continue to use, notice only has an indirect effect (through greater privacy policy effectiveness but not through trust).

This research also confirms that smart home speaker privacy policies are valued differently depending on user characteristics. Specifically, the findings show the

positive moderating effects of information sensitivity and information transparency on the effect of notice and choice on effectiveness of privacy policy and trust.

The thesis‘ results contain important lessons for both academics and practitioners. We now describe our study's theoretical and managerial implications in turn.

## 5.1. THEORETICAL IMPLICATIONS

In this section, the main theoretical contributions of the dissertation are highlighted. The contributions are differentiated between those to information privacy research, specific privacy theories, and the literature on anthropomorphising AI devices.

First, this dissertation contributes to information privacy research by examining how to eliminate or mitigate two key factors that create user concerns: covert information collection and perceived surveillance. These two factors are related to what is called passive listening.

Data collection is relevant for companies wanting to offer better personalised services to smart home speaker users. Previous research has paid little attention to covert data collection, instead of focusing on consumer responses to overt data collection (Aguirre et al., 2016; Libaque-Sáenz et al., 2021). This dissertation provided evidence that humanising smart home speakers, building trust, and creating social presence effectively improve user attitudes toward covert data collection.

Regarding perceptions of surveillance, users tend to think that smart home speakers are listening all the time. This creates the perception of being under surveillance, which, in turn, creates distrust toward the device and the company.

However, little is known about this kind of _surveillance‘, its negative consequences, and how to mitigate them. Prior research has mainly focused on intrusiveness (Benlian et al 2019; Lucia-Palacios and Pérez-López, 2021). The results have offered new insights into how humanisation can influence surveillance perceptions.

Second, the findings also highlight the relevance of trust as an antecedent to both (a) user attitudes toward (overt and covert) data collection and (b) intention to continue to use. Trust is the common factor in the three studies. The results demonstrated how it plays an important role in reducing user privacy concerns related to smart home speakers. Trust has been included in privacy research as a factor helping reduce privacy concerns when disclosing personal information (Bansal et al 2016; Beldad et al., 2011; Taddei and Contena, 2013). However, this thesis provides new evidence for trust‘s mediation between the perceived value of personalisation and intentions to continue using smart home speakers.

Third, the thesis also provided new evidence that can contribute to extant privacy research. Specifically, its findings contribute to academic work on the personalisation-privacy paradox and the privacy-trust-behavioural intention model.

Research related to the personalisation-privacy paradox has focused on consumer behaviour when companies request personal information (Dinev and Hart, 2006; Klumpe et al., 2020; Wang et al., 2019). However, this research has not necessarily addressed how users respond when companies collect personal information without requesting permission. This thesis offers new insights into how the primary benefit of disclosing personal information (receiving personalised messages) can affect attitudes toward both overt and covert data collection. In this study, it is adopted a post-

purchase perspective, which differs from the pre-purchase perspective commonly used in research related to the personalisation-privacy paradox.

The thesis‘ findings also contribute to the current understanding of the privacy-trust-behavioural intention model (Liu et al., 2005). It is demonstrated that notice and choice are effective trust-building factors, factors that also promote intentions to continue using smart home speakers. Companies use notice and choice as part of their overt information collection strategies. Research on privacy policies has mainly addressed websites and apps (Bornschein, et al., 2020; Chang et al., 2018; Liu et al., 2022; Obar and Oeldorf-Hirsch, 2020). However, little is known about the effects notice and choice have on consumer behaviour responses in the smart home speaker context.

Scholars have examined notice‘s and choice‘s direct effects on trust (Wu et al., 2012) and the effectiveness of privacy policy (Chang et al., 2018). The thesis has provided new evidence for how these tools influence consumers‘ intentions to continue using a product via privacy policy effectiveness. This research also highlights the mediating role that privacy policies‘ perceived effectiveness and trust play when it comes to notice, choice, and the intention to continue to use.

The dissertation has examined how two moderators – information sensitivity and the importance of information transparency – can influence notice‘s and choice‘s effects on trust in the privacy-trust-behavioural intention model. Scholars have examined information sensitivity as an antecedent to privacy concerns or as a moderator in studies of willingness to disclose personal information (Aiello et al., 2020; Bansal and Gefen, 2010; Kang et al., 2022; Mothersbaough et al., 2012; Rohm and Milne, 2004; Sun et al., 2022; Tao et al., 2024). However, little is known about how information sensitivity can influence privacy policies‘ impacts on consumer behaviour.

Study 3 generated findings that reveal how privacy policy effectiveness – as a trust-building tool – is greater when users are given a choice. This effect is especially strong for users who consider the collection of personal information by smart home to be sensitive. Prior research has mainly examined consumer perceptions of company transparency (Aiello et al., 2020; Chung et al., 2022; Kim et al., 2019; Sansome et al., 2024). However, little is known about how the value consumers give to information transparency influences privacy policies as trust-building mechanisms. The thesis has provided new evidence for the importance of information transparency as a personal condition that influences notice‘s impact on the effectiveness of privacy policies and trust.

Fourth, this dissertation contributes to the research on anthropomorphising AI devices, specifically work related to the uncanny valley theory and the parasocial relationship theory. Smart home speakers have some conversational capabilities, and users therefore often perceive them as human-like. This generates a change in the relevant human–computer interactions. The findings obtained confirm the importance of human-like characteristics for smart home speakers. We have shown how such characteristics improve attitudes toward covert data gathering through (a) increased trust in the service provider, (b) increased perceived social presence, and (c) reduced perceptions of surveillance. Previous studies have examined humanisation‘s influence on trust, social presence, and the emotional reactions it triggers. There has, however, been little research into humanisation‘s effects on negative aspects like intrusiveness or privacy risks (Benlian et al., 2019; Lavado-Nalvaiz et al., 2022). This thesis makes a contribution to extant scholarship by examining humanisation‘s effect on perceived surveillance.

The thesis has also provided evidence for the effect of anthropomorphism on trust. This can contribute to the debate about the existence (or nonexistence) of an uncanny valley in the smart home speaker context. Prior research has shown that over-humanisation can lead to confusion about a device‘s ‗humanness‘, generating distrust in both the smart home speaker and the service provider (Poushneh, 2021; Troshani et al., 2021). The thesis examines humanisation‘s role in building a trusting relationship with a service provider. It is also demonstrated that humanisation has a U-shaped effect on trust in the service provider. This suggests that the more humanised the device, the better it is. This result does not support theories like the realism maximisation theory or the uncanny valley theory. Nonetheless, this thesis sheds new light on the variables of humanisation and trust in the service provider. Up until now, studies using the realism maximisation theory or the uncanny valley theory have only been focused on analysing trust in humanised objects. The thesis adds the dimension of trust in service providers.

Finally, the thesis contributes to parasocial relationship theory by showing how social presence plays a salient role in mitigating perceptions of surveillance (a negative aspect usually associated with smart home speakers). Previous research on this theory has paid little attention to negative responses (except intrusiveness) (Benlian et al., 2019; Lucia-Palacios and Pérez-López, 2021). We have also presented evidence for a relationship between social presence and trust. Specifically, social presence plays an important mediating role between (a) humanisation and trust, (b) humanisation and perceived surveillance, and (c) humanisation, trust, and attitudes toward covert data collection. As such, the results suggest that social presence can significantly improve user attitudes toward covert data collection strategies.

## 5.2. MANAGERIAL IMPLICATIONS

Given its objectives, this dissertation has managerial and practical implications related to the development of smart devices and parts of the technology sector more broadly.

First, regarding improving user experiences with smart home speakers, service providers should offer users a personalised device experience. Users consider personalisation to be valuable, and it can, therefore, lead to continued use. Receiving personalised information improves user attitudes, regardless of whether the information is overtly or covertly collected. Valuable personalised information also reduces users‘ privacy concerns about perceived surveillance and covert data collection.

Second, users are generally not aware of which information is being collected, how much is being collected, when it is being collected, or how it is being stored. We have highlighted the importance of trust in mitigating users‘ negative attitudes toward covert data collection. Smart home speaker providers should, therefore, develop a trusting relationship with their customers. Ways to do so include (a) offering personalised services, (b) incorporating an option that reminds users when the speaker is turned on, and (c) informing users about how their personal information is collected, when it is being collected, which information is being collected, and where it is stored.

Trust in a service provider is crucial for improving user attitudes and ensuring continued smart device use. Providers of these devices and the associated services must prioritise developing a secure and transparent relationship with their users. Doing so can strengthen the relationship of trust between user and company. This can be achieved through implementing privacy and security policies guaranteeing that users‘ personal data is used appropriately.

Third, to enhance their privacy policies‘ effectiveness, companies should implement privacy notice and choice statements. Clearly informing users about these policies and letting them choose how their personal information is handled can engender trust in the device and the provider. This can, in turn, increase the intention to continue using the device. Implementing these strategies will allow companies and sellers of smart home speakers to increase their devices‘ usage rates and create a habit of consumption.

Fourth, privacy concerns, perceived risks, and the importance of privacy can vary among smart home speaker users. Companies should, therefore, identify user characteristics that can render privacy policies more, or less, effective. These characteristics include sensitivity to personal information collection and the importance given to information transparency. To this end, it might be beneficial for smart device companies to survey users when they first start using one of their devices.

Finally, there are also implications for smart home speaker developers and designers. When designing their interfaces, they should consider the degree of humanisation they want to achieve. Greater naturalness can be achieved when there is effective two-way communication between user and device. Incorporating these features will increase social presence and trust. It can also reduce perceived surveillance, which is a significant negative perception (one that can reduce levels of use, satisfaction, or recommendations to others). Adding human characteristics to smart home speakers can involve designing a more human-like voice, giving the device a human name, and creating the ability to engage in more humanised conversations. This can help build trusting relationships with users and thus foster a more positive attitude toward covert data collection practices.

## 5.3. LIMITATION AND FUTURE RESEARCH

Despite the above mentioned theoretical contributions and managerial implications, the thesis has some limitations. In this section, it is outlined the main limitations and suggested potential areas for future research. Exploring these areas can (a) enhance the understanding of privacy risks and trust-building strategies related to smart home speakers, (b) contribute to the topical literature, and (c) provide practical insights for managers.

Some limitations are related to the methodology it is employed. The methodology used in this dissertation is based on data obtained by surveying US smart home speaker users. In Study 3, experimental studies could be conducted with different privacy scenarios or user-provided tools. This might generate additional evidence and a deeper understanding of the relevant consumer behaviours and privacy concerns. Future research could empirically investigate which personal characteristics or company signals can help generate more efficient privacy policies and build trusting relationships with service providers.

In Study 2, latent variables explained humanisation and social presence. Experimentation could serve as a methodology for this study because the variables we used are sensitive and must be measured at the moment of use. Future research could analyse the humanisation variable at different levels to determine whether the results vary in tandem.

Another possible limitation is that the sample used was obtained from a single country, the US. It is, though, important to take cultural background into account when conducting the kind of studies we have engaged in some populations (e.g., the Japanese) are more accustomed to using smart technologies or are more willing to adopt new

technologies (especially when it comes to robotics) (Bröhl et al., 2019). Concerns about how personal information is collected, used, and stored might also vary from region to region. It would be informative to extend this research to other cultural contexts and compare the results. This could be of interest to companies and marketers when carrying out their sales and advertisement campaigns. It might also inform regulations related to personalised data collection practices and transparency about privacy policies. The results could also be of interest to designers when it comes to personalising device features (making them more, or less, human-like).

Another methodological aspect to consider is the data‘s cross-sectional nature. Future research could involve conducting longitudinal studies to analyse the evolution of surveillance perceptions and covert data collection practices as a function of user experiences with the device. This would provide more insights into user experiences throughout the consumer journey.

The results suggest that socio-demographic aspects are relevant (even if they have not been the focus of the studies). In Study 2, it is found that users with higher levels of education are more likely to have a positive attitude toward covert data collection than those with lower levels of education. Future research could assess whether education significantly influences users‘ tolerance for privacy risk. This could be mitigated by companies providing more education or by providing more warnings about their data collection strategies.

Regarding the gender control variable, it is used a binary measure: male/female. However, respondents might identify with neither of these options. Cartwright and Nancarrow (2022) have suggested that, although the number of respondents identifying as non-binary is currently low, it will increase as this identity becomes more socially

accepted. Future research could openly ask respondents the question to avoid feelings of exclusion.

Because the dissertation analysed the use of technological devices, age might be a key variable distinguishing different user behavioural patterns. Future research could replicate some of the proposed models and analyse how the results might vary according to age distributions.

The thesis has focused on the intention to continue to use as the primary behavioural response (especially in Studies 1 and 3). One could, however, take other consumer responses into account. These might have salient managerial implications. Future research could explore the impact of the value of personalised messages and privacy policy tools on (a) cognitive responses (e.g., satisfaction and recommendation) and (b) emotional responses (e.g., fatigue and stress).

In the thesis, it is considered three mechanisms for improving trust and reducing privacy concerns among smart home speaker users. One could, however, examine other factors that might explain consumer behaviour. Consumers could have certain prior expectations about how these devices collect information. It might, then, be interesting to determine how the confirmation or disconfirmation of these expectations affects user behaviour.

Lastly, the studies only focused on smart home speakers. The findings and managerial suggestions can, though, be cautiously extended to other contexts. New cars, for example, are equipped with voice control systems. A car is an intimate space where many conversations take place. Monitoring private conversations or private calls in the car will potentially give rise to the kind of privacy issues we have been discussing. The literature on this issue is relatively scarce (Kim and Heo, 2021; Tan et al., 2021). Future

studies could examine whether the findings are replicable in technological contexts that are similar to the smart home speaker context.

## REFERENCES


Aguirre, E., Roggeveen, A. L., Grewal, D., and Wetzels, M. (2016). The personalisation-privacy paradox: implications for new media. *Journal of Consumer Marketing*, *33*(2), 98-110.

Aiello, G., Donvito, R., Acuti, D., Grazzini, L., Mazzoli, V., Vannucci, V., & Viglia, G. (2020). Customers‘ willingness to disclose personal information throughout the customer purchase journey in retailing: The role of perceived warmth. *Journal of Retailing*, *96*(4), 490-506.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 13-28.

Bansal, G., Zahedi, F. M., & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems*, *24*, 624-644.

Benlian, A., Klumpe, J., & Hinz, O. (2020). Mitigating the intrusive effects of smart home assistants by using anthropomorphic design features: A multimethod investigation. *Information Systems Journal*, *30*(6), 1010-1042.

Bornschein, R., Schmidt, L., & Maier, E. (2020). The effect of consumers‘ perceived power and risk in digital information privacy: The example of cookie notices. *Journal of Public Policy & Marketing*, *39*(2), 135-154.

Bröhl, C., Nelles, J., Brandl, C., Mertens, A., & Nitsch, V. (2019). Human–robot collaboration acceptance model: development and comparison for Germany, Japan, China and the USA. *International Journal of Social Robotics*, *11*(5), 709-726.

Cartwright, T., and Nancarrow, C. (2022). A Question of Gender: Gender classification in international research. *International Journal of Market Research*, *64*(5), 575-593

Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers‘ perceived privacy. *Government Information Quarterly*, *35*(3), 445-459.

Chung, W. Y., Nam, J., Ryong, K., & Lee, D. (2022). When, how, and what kind of information should Internet service providers disclose? A study on the transparency that users want. *Telematics and Informatics*, *70*, 101799.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61-80.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295-316

Foehr, J., & Germelmann, C. C. (2020). Alexa, can I trust you? Exploring consumer paths to trust in smart voice-interaction technologies. *Journal of the Association for Consumer Research*, *5*(2), 181-205.

Gahler, M., Klein, J. F., & Paul, M. (2023). Customer experience: Conceptualization, measurement, and application in omnichannel environments. *Journal of Service Research*, *26*(2), 191-211.

Go, E., & Sundar, S. S. (2019). Humanizing chatbots: The effects of visual, identity and conversational cues on humanness perceptions. *Computers in Human Behaviour*, *97*, 304-316.

Gupta, R., Jain, K., & Jajodia, I. (2021). Determinants of smart speaker adoption intention: extending the theory of planned behaviour. *International Journal of Technology Marketing*, *15*(2-3), 181-202.

Horton, D., & Richard Wohl, R. (1956). Mass communication and para-social interaction: Observations on intimacy at a distance. *Psychiatry*, *19*(3), 215-229.

Kang, H., & Kim, K. J. (2022). Does humanization or machinization make the IoT persuasive? The effects of source orientation and social presence. *Computers in Human Behavior*, *129*, 107152.

Kim, J., & Heo, J. (2021) Please stop listening while i make a private call: Context-aware in-vehicle mode of a voice-controlled intelligent personal assistant with a privacy consideration. In *International Conference on Human-Computer Interaction,* 177-193. Cham: Springer International Publishing.

Kim, T., Barasz, K., & John, L. K. (2019). Why am I seeing this ad? The effect of ad transparency on ad effectiveness. *Journal of Consumer Research*, *45*(5), 906-932.

Klumpe, J., Koch, O. F., and Benlian, A. (2020). How pull vs. push information delivery and social proof affect information disclosure in location based services. *Electronic Markets*, *30*(3), 569-586.

Lavado-Nalvaiz, N., Lucia-Palacios, L., & Pérez-López, R. (2022). The Role of the Humanisation of Smart Home Speakers in the Personalisation–Privacy Paradox. *Electronic Commerce Research and Applications*, 53, 101146.

Libaque-Sáenz, C. F., Wong, S. F., Chang, Y., & Bravo, E. R. (2021). The effect of fair information practices and data collection methods on privacy-related behaviours: A study of mobile apps. *Information & Management*, *58*(1), 103284.

Liu, B., Miltgen, C. L., & Xia, H. (2022). Disclosure decisions and the moderating effects of privacy feedback and choice. *Decision Support Systems*, *155*, 113717.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S. (2005). Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, *42*(2), 289-304.

Lucia-Palacios, L., and Pérez-López, R. (2021). Effects of Home Voice Assistants' Autonomy on Instrusiveness and Usefulness: Direct, Indirect, and Moderating Effects of Interactivity. *Journal of Interactive Marketing*, *56*, 41-54.

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of service research*, *15*(1), 76-98.

MSI (2022). Marketing Science Instiurte Research Proprities (2022-2024). https://www.msi.org/wp-content/uploads/2022/10/MSI-2022-24-Research-Priorities-Final.pdf (access 26/12/2023)

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128-147.

Poushneh, A. (2021). Humanizing voice assistant: The impact of voice assistant personality on consumers‘ attitudes and behaviors. *Journal of Retailing and Consumer Services*, 58, 102283

Rohm, A. J., & Milne, G. R. (2004). Just what the doctor ordered: The role of information sensitivity and trust in reducing medical information privacy concern. *Journal of Business Research*, *57*(9), 1000-1011.

Sansome, K., Wilkie, D., & Conduit, J. (2024). Beyond information availability: Specifying the dimensions of consumer perceived brand transparency. *Journal of Business Research*, *170*, 114358.

Sun, S., Zhang, J., Zhu, Y., Jiang, M., & Chen, S. (2022). Exploring users' willingness to disclose personal information in online healthcare communities: the role of satisfaction. *Technological Forecasting and Social Change*, *178*, 121596.

Tan, Z., Dai, N., Su, Y., Zhang, R., Li, Y., Wu, D., & Li, S. (2021). Human–machine interaction in intelligent and connected vehicles: a review of status quo, issues, and opportunities. *IEEE Transactions on Intelligent Transportation Systems*, *23*(9), 13954-13975.

Tao, S., Liu, Y., & Sun, C. (2024). Understanding information sensitivity perceptions and its impact on information privacy concerns in e-commerce services: Insights from China. *Computers & Security*, *138*, 103646.

Troshani, I., Rao Hill, S., Sherman, C., & Arthur, D. (2021). Do we trust in AI? Role of anthropomorphism and intelligence. *Journal of Computer Information Systems*, *61*(5), 481-491.

Wang, Y., & Herrando, C. (2019). Does privacy assurance on social commerce sites matter to millennials?. *International Journal of Information Management*, *44*, 164-177.

# Resumen

## MOTIVACIÓN Y OBJETIVOS

En los últimos años, la Inteligencia Artificial (IA) se ha convertido en un tema de gran relevancia en el ámbito profesional y académico (Mehta et al., 2022; Vaid et al., 2023). Esto ha propiciado que las empresas hayan empezado a invertir en tecnología basada en IA con el objetivo de mejorar la experiencia del consumidor (Klaus y Zaichowsky, 2021). Una de estas tecnologías, son los altavoces inteligentes o asistentes de voz, los cuales emplean algoritmos de IA para mejorar continuamente su rendimiento y precisión a lo largo del tiempo y ofrecer conversaciones personalizadas basadas en información previa. Además contienen procesamiento de lenguaje natural (PLN) lo que les hace capaces de reconocer la voz, entender los comandos dados y responder a las peticiones de los usuarios a través de la conversación (Molinillo et al., 2023; Oliveira et al., 2023). Este es el caso de dispositivos como Google Home, Alexa de Amazon o HomePod de Apple.

El uso de altavoces inteligentes ha crecido considerablemente en los últimos años, y se espera que el mercado mundial de estos dispositivos crezca de 11.000 millones de dólares en 2022 a 100.000 millones en 2032[3]. Sin embargo, a pesar de que el uso de estos altavoces inteligentes ha aumentado considerablemente, también lo ha hecho la preocupación de los usuarios por su privacidad. Para recibir la información personalizada que comentábamos anteriormente, estos dispositivos recopilan, almacenan y comparten información personal (Frick et al., 2021). Esto tiene un impacto directo en las empresas, ya que la preocupación por la privacidad puede afectar directamente a sus ingresos si, por ejemplo, los consumidores deciden no comprar artículos a empresas que no respeten su privacidad (Baruh et al., 2017). Además, las

[3] Market.us' report (2023) https://market.us/report/smart-speaker-market/request-sample/

violaciones de la privacidad pueden afectar al valor de la marca y, posteriormente, al valor de la compañía (Checa, 2018).

En este aspecto, el *Marketing Science Institute (MSI)* (2022-2024) destacó la importancia de estudiar si la tecnología basada en IA, como los *chatbots*, asistentes virtuales y altavoces inteligentes entre otros, podrían aumentar o sustituir la atención a clientes convencional, y cómo puede llegar a afectar esto a la experiencia del cliente. En este sentido, la literatura académica aboga por estudiar los diferentes canales y contextos a través de los cuales los clientes se relacionan con las empresas (De Keyser et al., 2020; Gahler et al., 2023). Adicionalmente, el Ministerio de Ciencia e Innovación tiene como punto estratégico dentro del Plan Estatal de Investigación Científica, Técnica y de Innovación (2021-2023), elaborado por (MSI) el estudio del uso de la inteligencia artificial por parte de consumidores y organizaciones. El *Marketing Science Institute*, estableció como prioridad de investigación para el periodo 2022-2024 la preocupación por la privacidad de los consumidores, ya que puede constituir un freno para el avance de la inteligencia artificial y sus beneficios para las empresas.

La privacidad se rhacerre a la evaluación del usuario acerca del acceso que otros agentes (como empresas, personas, gobiernos u otras entidades) tienen sobre su informatión personal (Dinev et al., 2013), y surge como una de las principales preocupaciones y riesgos de los usuarios dentro del contexto de los productos inteligentes. Los altavoces domésticos inteligentes pueden realizar una amplia variedad de tareas, como consultar los eventos programados en el calendario, repro193icien música, pedir comida o controlar otros dispositivos domésticos inteligentes siguiendo una orden verbal o escrita (Chatterjee y Karahanna, 2019; Gao y Liu, 2022). Al mismo tiempo, se utilizan para responder a las peticiones de los usuarios de forma personalizada y para recopilar información sobre su comportamiento, hábitos de

consumo, gustos y preferencias, así como sobre el entorno en el que se desenvuelven (Mogaji et al., 2020; Kumar et al., 2019). Para que este servicio personalizado funcione de forma adecuada, es necesario obtener información personal de los usuarios. Cuando h194iciendo194ón recogida de información, la literatura existente distingue dos tipos en función de la transparencia con la que se lleva a cabo: abierta y encubierta (Xu et al., 2011). Los estudios anteriores se han centrado en examinar la situación en la que las empresas piden permiso para recopilar información (recopilación abierta). En esta recopilación abierta, la empresa notifica a los consumidores que se está produciendo recogida de información personal, lo que genera sentimientos de confianza, transparencia y fiabilidad hacia la empresa y control sobre la información facilitada (Libaque-Sáenz et al. 2021). Por el contrario, cuando la información se recoge de forma encubierta, los consumidores no son conscientes de que se está produciendo dicha recogida o no se les notifica de forma explícita (Aguirre et al. 2015; Hayes et al. 2021; Xu et al. 2011). En este contexto, los usuarios evalúan racionalmente la diferencia entre costes y beneficios derivados de esta personalización, y utilizan este cálculo como base para la toma de decisiones, lo que se conoce como Teoría del cálculo de la privacidad (Culnan y Armstrong, 1999).

Asimismo, los dispositivos están equipados con micrófonos que están constantemente alerta, esperando la palabra o comando que les active, por lo que están escuchando constantemente las conversaciones a su alrededor. Esto plantea cuestiones muy delicadas en relación con la vigilancia percibida y el intrusismo.

Por todo ello, la privacidad es un aspecto relevante para los usuarios que las empresas deben controlar y conocer, de forma que puedan ofrecer una buena experiencia al cliente y ser más exitosas. En este sentido, las compañías se han venido preocupando por generar una mayor confianza entre los usuarios (Pitardi y Marriott,

2021) para que éstos perciban positivamente la recogida de información personal. En consecuencia, el objetivo de esta Tesis Doctoral es estudiar cómo las empresas pueden generar confianza y reducir las consecuencias negativas de la percepción de pérdida de privacidad debido a la recogida de información y así enfatizar el mayor uso continuado de los altavoces inteligentes. Para ello, y con el ánimo de contribuir a la literatura existente, la Tesis propone tres mecanismos que pueden aumentar la confianza de los usuarios y afectar a sus percepciones de pérdida de privacidad: 1) fomentar los servicios personalizados, 2) invertir en una mayor humanización de las interacciones con los usuarios, y 3) aumentar la transparencia y el control percibido por los mismos.

En cuanto a la personalización del servicio, y dado que la recogida previa de información es su premisa básica, las investigaciones existentes se han centrado en la disposición que tienen los consumidores a la hora de revelar información cuando la recogida se produce de forma abierta. Sin embargo, pocas de ellas se han centrado en el comportamiento de los usuarios cuando la información se recopila de forma encubierta. En este caso, a menudo los consumidores son conscientes de esa recogida cuando empiezan a recibir anuncios personalizados sin haber realizado previamente una búsqueda sobre ese producto. Aunque el efecto de la personalización de los mensajes puede superar los riesgos de privacidad asociados a revelar su información personal (Xu et al., 2011), no está claro el efecto que tiene sobre la actitud de los consumidores hacia la recogida encubierta de información. En este caso los usuarios tienen una sensación no solo de invasión y pérdida de privacidad, sino también de pérdida de control sobre sus datos (Hayes et al., 2021), así como una percepción de vigilancia (Kowalczuk 2018). Dado que se sabe poco sobre las actitudes de los usuarios hacia la forma en que se recopila su información personal, sus antecedentes y consecuencias, esta Tesis Doctoral propone estudiar en mayor profundidad dichos aspectos.

En relación con el segundo de los mecanismos propuestos, la literatura sobre IA, ha encontrado que la humanización de los dispositivos influye en las emociones, percepciones y comportamiento de los consumidores (Foehr y Gemelman 2020; Cherif y Lemoine, 2019; Blut et al 2021). Dentro de esta literatura, se observan tres teorías como las más relevantes. En primer lugar, la Teoría de la Maximización del Realismo (Groom et al., 2009) demuestra que un diseño con características humanas provoca emociones positivas en los consumidores, debido a que pueden establecer una conexión natural y personal con el agente no humano, generando una sensación de familiaridad (Mende et al., 2019; Toader et al., 2019). En segundo lugar, la Teoría de las Relaciones Parasociales (Horton y Wohl, 1956), sobre la que se fundamenta la anterior, propone que la humanización aumenta la credibilidad de los mensajes (Foehr y Germelmann, 2020; Martin et al., 2020; Poushneh, 2021), e incrementa la presencia social (Chérif y Lemoine, 2019; Kang y Kim, 2022), generando relaciones de confianza y cercanía como las que se pueden dar entre amigos (Pitardi y Marriott, 2021) y reduciendo la intrusividad percibida (Benlian et al., 2019). En tercer lugar, la Teoría del Valle Misterioso (Mori et al., 2012) sugiere que la humanización tiene un efecto cúbico en la respuesta emocional de los usuarios. Esto significa que para niveles bajos pero crecientes de humanización, los usuarios generan afinidad hacia el dispositivo, hasta llegar a un punto de humanización en el que empieza a ser percibido como extraño y perturbador (Mathur et al., 2020).

Dado que la humanización o antropomorfismo puede generar mayor afinidad y aumentar la presencia social, también puede ser un atributo relevante para generar confianza en el usuario, así como para mejorar su actitud hacia la recogida de información. Estas relaciones no han sido analizadas en profundidad en la literatura

previa y es por ello que la presente Tesis Doctoral pretende arrojar luz sobre estas relaciones en el contexto de los altavoces inteligentes.

En tercer lugar, para que las empresas y proveedores de servicios puedan reducir los riesgos de privacidad y la sensación de intrusismo de los usuarios, así como aumentar su confianza, deben considerarse las políticas de privacidad que llevan a cabo y cómo las comunican a los consumidores (Yang et al., 2020). La literatura previa ha discutido la importancia de proporcionar políticas de privacidad basadas en el uso de notificaciones y opciones de elección para generar confianza en los usuarios (Wu, 2012; Chang, 2018). Sin embargo, hay muy poca literatura que se centre en explorar si estas herramientas de privacidad (notificaciones y opciones de elección) tienen impacto en la creación de confianza. Además, tampoco se han detectado en la literatura estudios que analicen si los efectos de estas herramientas de privacidad varían en función de la actitud del consumidor hacia la recogida de información, esto es, cómo de sensible es ante la recogida de información y qué importancia otorgan a la transparencia en dicha recogida. Investigaciones anteriores han descubierto que la eficacia de la política de privacidad contribuye a generar confianza (Guo et al., 2022), pero ningún estudio ha analizado si esta relación puede verse afectada por la importancia que para el usuario tiene la transparencia de la información. Por ello, el análisis de los efectos de las notificaciones y opciones de elección sobre privacidad que emiten los altavoces inteligentes en la confianza de los usuarios, así como las diferencias en función de sus actitudes constituye una importante oportunidad de investigación.

En base a estas oportunidades de investigación, tal y como se ha mencionado anteriormente, el principal objetivo de esta Tesis Doctoral es desarrollar una comprensión integral de las diversas formas que existen para reducir los riesgos de privacidad asociados al uso de altavoces domésticos inteligentes y, al mismo tiempo,

orientar a las empresas y desarrolladores para que mejoren sus relaciones con los usuarios de estos dispositivos. Para cumplir este objetivo, la Tesis está compuesta por tres estudios empíricos que se detallan a continuación.

## ESTUDIOS EMPÍRICOS

El **primer estudio empírico** pretende analizar de qué manera influye la personalización que los altavoces inteligentes ofrecen en la actitud de los usuarios hacia la recogida de información, distinguiendo entre recopilación abierta y encubierta. Además, este estudio se centra en examinar el efecto de la actitud de los usuarios hacia la recogida de información abierta y encubierta sobre la intención de seguir utilizando el dispositivo. El papel mediador que ejerce la confianza en la relación entre las actitudes de los consumidores y la intención de seguir utilizando el dispositivo también es analizado. Este estudio se enmarca en la Teoría del Cálculo de la Privacidad y la Paradoja de la Personalización-Privacidad (Culnan y Armstrong, 1999; Dinev y Hart, 2006; Xu et al., 2011). Se explora si el valor de recibir información personalizada puede determinar las actitudes hacia dos tipos diferentes de recogida de información por parte del proveedor del servicio y si, además, puede crear una relación de confianza entre usuarios y proveedores. Las hipótesis de la investigación se comprobaron con los datos recogidos mediante una encuesta administrada a través de Mechanical Turk (MTurk). Todos los participantes son estadounidenses, mayores de 18 años, poseen un altavoz doméstico inteligente y el inglés es su lengua materna. Aunque inicialmente se obtuvieron 700 respuestas, algunos cuestionarios fueron eliminados porque las respuestas de los encuestados seguían un patrón o respondían incorrectamente a una de las preguntas de control. Esto arrojó un total de 679 respuestas válidas. El modelo se estimó aplicando ecuaciones estructurales. Los resultados muestran que el valor de la

personalización de los mensajes mejora la actitud de los usuarios hacia ambos tipos de recogida de información (abierta y encubierta). Este estudio demuestra el importante papel que desempeña la confianza en la gestión de la información ya que se encuentra una relación positiva entre el valor de la personalización y la confianza, así como entre la confianza y la intención de seguir utilizándola.

**El segundo estudio empírico** analiza si la humanización de los altavoces inteligentes puede mejorar la actitud de los usuarios hacia la recigida encubierta de información y generar confianza. Además, estudia si dicha humanización puede influir en la reducción de la percepción de vigilancia ejercida por estos dispositivos, centrándose en las ventajas que pueden ejercer en términos de presencia social. Para abordar estos objetivos, se desarrolla un marco teórico basado en la literatura sobre humanización y concretamente las tres teorías mencionadas anteriormente (Teoría de la Maximización del Realismo, Teoría del Valle Misterioso y Teoría de las Relaciones Parasociales). Al igual que en el estudio anterior, se emplea una metodología de ecuaciones estructurales. La muestra obtenida es la misma que la del estudio anterior y consiste en 679 usuarios estadounidenses mayores de 18 años que poseen un altavoz inteligente en casa. Los resultados revelan que la humanización percibida ayuda a aumentar los sentimientos de presencia social y también mejora la actitud de los usuarios hacia la recogida encubierta de información. También se demuestra que la humanización influye negativamente en la confianza cuando dicha humanización es muy baja. Sin embargo, llega un punto de humanización a partir del cual su influencia es positiva. Además, se demuestra que la humanización tiene un impacto negativo en la percepción de la vigilancia. Por último, esta investigación concluye que si el usuario confía en la empresa que ofrece el servicio, su actitud hacia la recogida de información

será positiva, aunque los usuarios puedan pensar que la información se haya recogido de forma encubierta.

El **tercer estudio empírico** analiza cómo las notificaciones y las opciones de elección, como herramientas de la política de privacidad de las empresas, pueden mejorar la confianza en los proveedores de altavoces domésticos inteligentes. Además, examina el papel de dos tipos de actitudes (el grado de sensibilidad a la información personal y la importancia de la transparencia informativa), sobre el efecto que tienen las notificaciones y las opciones de elección en la eficacia de las políticas de privacidad y en la confianza. Este estudio se basa en el modelo Privacidad-Confianza-Intención de comportamiento propuesto por Liu (2005), y para comprobar las hipótesis propuestas se utiliza de nuevo una metodología basada en ecuaciones estructurales aplicada a una muestra de 679 usuarios estadounidenses de altavoces domésticos inteligentes. Los resultados confirman el modelo Privacidad-Confianza-Intención de comportamiento, que sugiere que la notificación tiene un efecto directo e indirecto sobre la confianza, mediado por la eficacia de la política de privacidad. Por otro lado, las opciones de elección sólo tienen un efecto indirecto total sobre la confianza. Esta investigación también confirma que la política de privacidad de los altavoces domésticos inteligentes puede valorarse de forma diferente en función de las características o actitudes de los usuarios. En concreto, se demuestra el efecto moderador positivo de la sensibilidad a la información personal y la transparencia informativa sobre el impacto de las notificaciones y de las opciones de elección en la eficacia de la política de privacidad y en la confianza.

# Conclusiones

## CONTRIBUCIONES TEÓRICAS

La presente Tesis Doctoral realiza una serie de contribuciones teóricas a la literatura existente, concretamente es posible diferenciar la literatura sobre privacidad, las teorías de privacidad y las teorías de antropomorfismo o humanización.

Esta Tesis Doctoral contribuye examinando cómo eliminar o mitigar dos aspectos principales que generan preocupación en los usuarios: la recogida encubierta de información y la percepción de vigilancia. Hasta la fecha, todas las investigaciones existentes se han centrado en la respuesta del consumidor a la recogida de información manifiesta (Aguirre et al., 2016; Libaque-Sáenz et al., 2021). Con esta Tesis Doctoral se aportan nuevas evidencias sobre cómo mejorar la actitud del usuario hacia la recopilación de información encubierta. Respecto a vigilancia percibida, los usuarios sienten que los altavoces inteligentes están todo el tiempo escuchando a través de sus micrófonos, por lo que se sienten vigilados, generando desconfianza hacia el dispositivo y la empresa. Sin embargo, poco se sabe sobre estas consecuencias negativas y cómo se puede ayudar a reducirlas. En este sentido, esta Tesis Doctoral ofrece nuevas perspectivas sobre cómo la humanización puede influir en las percepciones de la vigilancia. La confianza es el factor común en los tres estudios. A lo largo de esta tesis se demuestra su importante papel en la reducción de las preocupaciones de privacidad que los usuarios tienen con el uso de los altavoces domésticos inteligentes. Aunque la confianza ha sido incluida previamente en la investigación sobre privacidad como un factor que ayuda a reducir la preocupación por la privacidad a la hora de revelar información personal (Bansal et al 2016; Beldad et al., 2011; Taddei y Contena, 2013), nuestro estudio aporta nuevas evidencias sobre el papel mediador de la confianza entre el valor percibido de la personalización y la intención de seguir utilizando altavoces domésticos inteligentes. Además, el estudio aborda el papel de la confianza como

moderador en la relación indirecta entre el valor de la personalización y el uso continuado, a través de la actitud hacia la recopilación encubierta de información.

Esta Tesis Doctoral también contribuye a teorías específicas relacionadas con la investigación sobre la privacidad. En concreto, nuestros resultados contribuyen a la Paradoja de la Personalización-Privacidad y al modelo Privacidad-Confianza-Intención de comportamiento. Las investigaciones enmarcadas en la Paradoja de la Personalización-Privacidad han analizado el comportamiento de los consumidores cuando las empresas solicitan información personal (Dinev y Hart, 2006; Klumpe et al., 2020; Wang et al., 2019). Sin embargo, estas investigaciones no han analizado la forma en que los usuarios responden cuando las empresas recopilan información personal sin solicitar permiso para ofrecerles un servicio personalizado. Por lo tanto, esta tesis ofrece perspectivas sobre cómo el principal beneficio de revelar información personal (recibir mensajes personalizados) puede actuar como un antecedente de las actitudes hacia la recopilación de información tanto abierta como encubierta.

En lo que respecta al modelo Privacidad-Confianza-Intención de comportamiento (Liu et al., 2005) se demuestra claramente que la notificación y las opciones de elección son factores eficaces para generar confianza que también promueven la intención de seguir utilizando altavoces domésticos inteligentes. Hasta la fecha, la investigación sobre políticas de privacidad ha abordado principalmente el contexto de sitios web y apps (Bornschein, et al., 2020; Chang et al., 2018; Liu et al., 2022; Obar y Oeldorf-Hirsch, 2020). Sin embargo, poco se sabe sobre el efecto que la notificación y las opciones de elección tienen en las respuestas de comportamiento de los consumidores en el contexto de los altavoces domésticos inteligentes.

Adicionalmente, aportamos nuevas pruebas de cómo la notificación y las opciones de elección, a través de la eficacia de la política de privacidad y la confianza, influyen en la intención de los consumidores de seguir utilizando el producto. Destacamos el papel mediador de la eficacia percibida de la política de privacidad y la confianza entre el aviso y la elección y la intención de seguir utilizando el producto. Además, esta Tesis Doctoral examina cómo la sensibilidad a la información y la importancia de la transparencia informativa pueden influir en el modo en que la notificación y la elección afectan a la confianza. En este sentido, se contribuye con nuevos hallazgos que revelan que la eficacia de la política de privacidad como herramienta de creación de confianza es mayor cuando se da a los usuarios la posibilidad de elegir, y que este efecto es particularmente fuerte para los usuarios que perciben que la información recopilada por el altavoz doméstico inteligente es sensible. Además, esta tesis aporta nuevas pruebas de la importancia que los usuarios conceden a la transparencia de la información como otra condición personal que influye en el impacto del aviso sobre la eficacia de la política de privacidad y la confianza.

Esta Tesis demuestra que las características similares a las humanas que presentan estos dispositivos mejoran las actitudes hacia la recopilación de información encubierta a través de una mayor confianza en el proveedor, una mayor presencia social percibida y una menor vigilancia percibida. Aunque estudios anteriores han examinado la influencia de la humanización en la confianza, la presencia social y las reacciones emocionales que desencadena, pocas investigaciones han indagado en los efectos de la humanización sobre aspectos negativos como la intrusividad o los riesgos para la privacidad (Benlian et al., 2019; Lavado-Nalvaiz et al., 2022).

Adicionalmente se contribuye al debate sobre la existencia o no de un valle inquietante en el contexto de los altavoces domésticos inteligentes. Nuestra

investigación muestra que la humanización tiene un efecto en forma de U sobre la confianza en el proveedor de servicios, lo que sugiere que cuanto más humanizado está el dispositivo, mejor es. Este resultado no respalda teorías anteriores como la Teoría de la Maximización del Realismo o la teoría del Valle Misterioso (Poushneh, 2021; Troshani et al., 2021) pero se aporta una nueva visión con respecto a las variables de humanización y confianza en el proveedor de servicios.

En esta misma línea, se contribuye a la Teoría de las Relaciones Parasociales desarrollada por Horton y Wohl (1956) al demostrar que la presencia social desempeña un papel relevante a la hora de mitigar las percepciones de vigilancia, un aspecto negativo que suele asociarse a los altavoces inteligentes. Investigaciones previas sobre esta teoría habían prestado poca atención a las respuestas negativas, a excepción de la intrusividad (Benlian et al., 2019; Lucia-Palacios y Pérez-López, 2021). Además, esta Tesis Doctoral ofrece más evidencias del importante papel mediador que tiene la presencia social entre la humanización y la confianza, entre la humanización y la vigilancia percibida, y entre la humanización, la confianza y la actitud hacia la recogida encubierta de información.

## IMPLICACIONES PRÁCTICAS

Desde el punto de vista de las implicaciones prácticas, este estudio tiene implicaciones tanto para las compañías como para los desarrolladores de estos dispositivos inteligentes.

Por un lado las compañías deben ofrecer a los usuarios una experiencia personalizada, ya que se ha demostrado que el valor de recibir información personalizada genera una mayor continuidad de uso y, lo que es aún más importante,

mejora la actitud de los usuarios, independientemente de cómo se recopile su información privada. Los resultados muestran distintas formas en que los profesionales del marketing y las empresas pueden mejorar la actitud de los usuarios hacia la información encubierta. Por un lado, se demuestra la importancia de la confianza en el proveedor de servicios para mejorar la actitud de los usuarios hacia la recogida encubierta de datos. Esta confianza puede generarse mediante la reducción de anuncios intrusivos o con recomendaciones periódicas que recuerden a los usuarios que los altavoces están encendidos.

Además, los proveedores de estos dispositivos y servicios deben desarrollar una transparencia sólida y segura, así como políticas de privacidad y seguridad que garanticen a los usuarios que la empresa está haciendo un uso adecuado de sus datos personales, independientemente de cómo se recojan. En esta línea, las empresas deberían implementar notificaciones y opciones de elección como parte de sus políticas de privacidad, ya que pueden aumentar la eficacia de la política de privacidad y, por tanto, la confianza, así como la intención de seguir utilizando el altavoz doméstico inteligente. Adicionalmente, las empresas deberían detectar el tipo de usuarios de sus dispositivos en términos de sensibilidad a la información e importancia de la transparencia informativa, ya que estas características individuales influyen en la notificación y la elección y la percepción de una política de privacidad más efectiva.

En lo que respecta al diseño de los altavoces, se debe prestar atención a la hora de dotarlos de características similares a las humanas, como un lenguaje más natural o una interacción más humana. Esto, aumentará la presencia social y generará sentimientos de cercanía, reduciendo la vigilancia percibida, aumentando la confianza y mejorando la actitud de los usuarios.

## LIMITACIONES Y FUTURAS LINEAS DE INVESTIGACIÓN

A pesar de las contribuciones teóricas relevantes y las implicaciones prácticas, ninguna investigación está exenta de limitaciones. Sin embargo, estas limitaciones brindan oportunidades para futuras investigaciones.

En primer lugar, en lo que concierne a la metodología empleada, esta Tesis Doctoral ha empleado la encuesta como forma de recopilar información. Sin embargo, haber realizado diseños experimentales con distintos escenarios de privacidad habría proporcionado una comprensión más profunda del comportamiento de los consumidores y de sus preocupaciones en materia de privacidad. Del mismo modo, los efectos de la humanización y la presencia social sobre la actitud y el comportamiento de los usuarios podrían haberse medido a través de la experimentación. Por lo tanto, es interesante que futuras investigaciones puedan emplear esta metodología y comprobar si los resultados obtenidos en este estudio son robustos.

Otra limitación de esta Tesis Doctoral es que se ha realizado solamente con datos de usuarios estadounidenses. Sin embargo, el contexto cultural es un elemento realmente importante a tener en cuenta cuando hablamos de productos tecnológicos. Igualmente, las preocupaciones por la privacidad y por la recogida de información personal pueden variar de un país a otro. Por ello, futuras investigaciones podrían desarrollar esta misma investigación en diferentes contextos culturales y analizar si existen diferencias culturales. Esto podría ser de gran interés para las empresas y los profesionales del marketing a la hora de llevar a cabo diferentes campañas de marketing.

Otro aspecto metodológico relevante es la naturaleza transversal de los datos. Para conocer mejor la experiencia del usuario a lo largo de su recorrido como

consumidor, futuras investigaciones podrían realizar estudios longitudinales. De este modo es posible analizar la evolución de las percepciones de la vigilancia y la recopilación de información de forma encubierta a lo largo del tiempo y determinar si varía en función de la experiencia del usuario con el dispositivo.

En segundo lugar, respecto a las variables sociodemográficas, la variable de control sexo, se utilizó una medida binaria (hombre/mujer). Sin embargo, en la actualidad existe más de una opción con la que los usuarios pueden sentirse identificados. Por lo tanto, en futuras investigaciones se podría formular la pregunta sexo o genero de forma abierta o ampliando a más opciones de las propuestas en esta presente tesis. Dado que la tesis analiza el uso de dispositivos tecnológicos, la edad puede ser una variable determinante. Por ello, futuras investigaciones podrían replicar algunos de los modelos propuestos y analizar cómo pueden variar los resultados en función de diferentes distribuciones de edad.

En tercer lugar, las variables dependientes empleadas se han centrado en la intención de continuar empleado el producto como respuesta conductual del consumidor. Sin embargo futuras líneas de investigación podrían analizar otras respuestas cognitivas, como la satisfacción con el producto o la intención de recomendarlo, así como en respuestas emocionales, como la fatiga, el estrés o la ansiedad. Asimismo, esta tesis ha considerado tres mecanismos de creación de confianza que pueden reducir la preocupación por la privacidad entre los usuarios de altavoces inteligentes. Sin embargo, podría ser interesante examinar otros aspectos que pueden explicar el comportamiento de los consumidores como las experiencias que han tenido previamente con el uso de estos dispositivos.

Por último, nuestros estudios se han centrado en el contexto de los altavoces domésticos inteligentes. Sin embargo, existen otros muchos contextos donde se plantean problemas de privacidad similares. Por ejemplo los sistemas de control por voz de los coches. Al igual que los hogares, los coches son un espacio íntimo en el que tienen lugar muchas conversaciones, por lo que vigilar conversaciones privadas o llamadas privadas puede dar lugar a problemas de privacidad entre los usuarios. Futuras investigaciones podrían examinar si las conclusiones obtenidas en esta tesis pueden confirmarse en otros contextos.

## REFERENCIAS


Aguirre, E., Roggeveen, A. L., Grewal, D., & Wetzels, M. (2016). The personalisation-privacy paradox: implications for new media. *Journal of Consumer Marketing*, *33*(2), 98-110.

Bansal, G., Zahedi, F. M., & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems*, *24*, 624-644.

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26-53.

Beldad, A., De Jong, M., & Steehouder, M. (2011). I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions. *Computers in Human Behavior*, *27*(6), 2233-2242.;

Benlian, A., Klumpe, J., & Hinz, O. (2020). Mitigating the intrusive effects of smart home assistants by using anthropomorphic design features: A multimethod investigation. *Information Systems Journal*, *30*(6), 1010-1042.

Blut, M., Wang, C., Wünderlich, N. V., & Brock, C. (2021). Understanding anthropomorphism in service provision: a meta-analysis of physical robots, chatbots, and other AI. *Journal of the Academy of Marketing Science*, *49*(4), 632-658.

Bornschein, R., Schmidt, L., & Maier, E. (2020). The effect of consumers‘ perceived power and risk in digital information privacy: The example of cookie notices. *Journal of Public Policy & Marketing*, *39*(2), 135-154.

Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers‘ perceived privacy. *Government Information Quarterly*, *35*(3), 445-459.

Checa, A. A. T. (2018). *Talking about surveillance and human rights: how the Mexican press discussed the Gobierno Espia investigation*.

Chérif, E., & Lemoine, J. F. (2019). Anthropomorphic virtual assistants and the reactions of Internet users: An experiment on the assistant‘s voice. *Recherche et Applications en Marketing (English Edition)*, *34*(1), 28-47.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, *10*(1), 104-115.

De Keyser, A., Verleye, K., Lemon, K. N., Keiningham, T. L., & Klaus, P. (2020). Moving the customer experience field forward: introducing the touchpoints, context, qualities (TCQ) nomenclature. *Journal of Service Research*, *23*(4), 433-455.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295-316

Foehr, J., & Germelmann, C. C. (2020). Alexa, can I trust you? Exploring consumer paths to trust in smart voice-interaction technologies. *Journal of the Association for Consumer Research*, *5*(2), 181-205.

Frick, N. R., Wilms, K. L., Brachten, F., Hetjens, T., Stieglitz, S., & Ross, B. (2021). The perceived surveillance of conversations through smart devices. *Electronic commerce research and applications*, *47*, 101046.

Gahler, M., Klein, J. F., & Paul, M. (2023). Customer experience: Conceptualization, measurement, and application in omnichannel environments. *Journal of Service Research*, *26*(2), 191-211.

Gao, L., Waechter, K. A., & Bai, X. (2015). Understanding consumers‘ continuance intention towards mobile purchase: A theoretical framework and empirical study–A case of China. *Computers in Human Behavior*, *53*, 249-262

Groom, V., Nass, C., Chen, T., Nielsen, A., Scarborough, J. K., & Robles, E. (2009). Evaluating the effects of behavioral realism in embodied agents. *International Journal of Human-Computer Studies*, *67*(10), 842-849.

Guo, Y., Wang, X., & Wang, C. (2022). Impact of privacy policy content on perceived effectiveness of privacy policy: the role of vulnerability, benevolence and privacy concern. *Journal of Enterprise Information Management*, *35*(3), 774-795.

Hayes, J. L., Brinson, N. H., Bott, G. J., & Moeller, C. M. (2021). The Influence of Consumer–Brand Relationship on the Personalized Advertising Privacy Calculus in Social Media. *Journal of Interactive Marketing*, *55*, 16-30.

Horton, D., & Richard Wohl, R. (1956). Mass communication and para-social interaction: Observations on intimacy at a distance. *Psychiatry*, *19*(3), 215-229.

Kang, H., & Kim, K. J. (2022). Does humanization or machinization make the IoT persuasive? The effects of source orientation and social presence. *Computers in Human Behavior*, *129*, 107152.

Klaus, P., & Zaichkowsky, J. L. (2022). The convenience of shopping via voice AI: Introducing AIDM. *Journal of Retailing and Consumer Services*, *65*, 102490.

Klumpe, J., Koch, O. F., & Benlian, A. (2020). How pull vs. push information delivery and social proof affect information disclosure in location based services. *Electronic Markets*, *30*(3), 569-586.

Kowalczuk, P. (2018). Consumer acceptance of smart speakers: a mixed methods approach. *Journal of Research in Interactive Marketing*, *12*(4), 418-431.

Lavado-Nalvaiz, N., Lucia-Palacios, L., & Pérez-López, R. (2022). The Role of the Humanisation of Smart Home Speakers in the Personalisation–Privacy Paradox. *Electronic Commerce Research and Applications*, 53, 101146.

Libaque-Sáenz, C. F., Wong, S. F., Chang, Y., & Bravo, E. R. (2021). The effect of fair information practices and data collection methods on privacy-related behaviours: A study of mobile apps. *Information & Management*, *58*(1), 103284.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S. (2005). Beyond concern a privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, *42*(2), 289-304.

Liu, B., Miltgen, C. L., & Xia, H. (2022). Disclosure decisions and the moderating effects of privacy feedback and choice. *Decision Support Systems*, *155*, 113717.

Lucia-Palacios, L., & Pérez-López, R. (2021). Effects of home voice assistants' autonomy on instrusiveness and usefulness: direct, indirect, and moderating effects of interactivity. *Journal of Interactive Marketing*, *56*, 41-54.

Mathur, M. B., Reichling, D. B., Lunardini, F., Geminiani, A., Antonietti, A., Ruijten, P. A., & Szuts, A. (2020). Uncanny but not confusing: Multisite study of perceptual category confusion in the Uncanny Valley. *Computers in Human Behavior*, *103*, 21-30.

Mehta, P., Jebarajakirthy, C., Maseeh, H. I., Anubha, A., Saha, R., & Dhanda, K. (2022). Artificial intelligence in marketing: A meta-analytic review. *Psychology & Marketing*, *39*(11), 2013-2038.

Mende, M. A., Fischer, M. H., & Kühne, K. (2019). The use of social robots and the uncanny valley phenomenon. *AI love you: developments in human-robot intimate relationships*, 41-73.

Mogaji, E., Soetan, T. O., & Kieu, T. A. (2020). The implications of artificial intelligence on the digital marketing of financial services to vulnerable customers. *Australasian Marketing Journal*, *29*(3), 235-242

Molinillo, S., Rejón-Guardia, F., Anaya-Sánchez, R., & Liébana-Cabanillas, F. (2023). Impact of perceived value on intention to use voice assistants: The moderating effects of personal innovativeness and experience. *Psychology & Marketing*, *40*(11), 2272-2290.

Mori, M., MacDorman, K. F., & Kageki, N. (2012). The uncanny valley [from the field]. *IEEE Robotics & Automation Magazine*, *19*(2), 98-100.

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128-147.

Oliveira, G. G., Lizarelli, F. L., Teixeira, J. G., & de Sousa Mendes, G. H. (2023). Curb your enthusiasm: Examining the customer experience with Alexa and its marketing outcomes. *Journal of Retailing and Consumer Services*, *71*, 103220.)

Pitardi, V., & Marriott, H. R. (2021). Alexa, she's not human but… Unveiling the drivers of consumers' trust in voice-based artificial intelligence. *Psychology & Marketing*, *38*(4), 626-642.

Poushneh, A. (2021). Humanizing voice assistant: The impact of voice assistant personality on consumers‘ attitudes and behaviors. *Journal of Retailing and Consumer Services*, 58, 102283

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure?. *Computers in human behavior*, *29*(3), 821-826.

Toader, D. C., Boca, G., Toader, R., Măcelaru, M., Toader, C., Ighian, D., & Rădulescu, A. T. (2019). The effect of social presence and chatbot errors on trust. *Sustainability*, *12*(1), 256.

Troshani, I., Rao Hill, S., Sherman, C., & Arthur, D. (2021). Do we trust in AI? Role of anthropomorphism and intelligence. *Journal of Computer Information Systems*, *61*(5), 481-491.

Vaid, S., Puntoni, S., & Khodr, A. (2023). Artificial intelligence and empirical consumer research: A topic modeling analysis. *Journal of Business Research*, *166*, 114110.

Wang, Y., & Herrando, C. (2019). Does privacy assurance on social commerce sites matter to millennials?. *International Journal of Information Management*, *44*, 164-177.

Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in human behavior*, *28*(3), 889-897.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalisation privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*(1), 42-52.

Yang, Q., Gong, X., Zhang, K. Z., Liu, H., & Lee, M. K. (2020). Self-disclosure in mobile payment applications: Common and differential effects of personal and proxy control enhancing mechanisms. *International Journal of Information Management*, *52*, 102065.