Leschanowsky, Anna ; Rech, Silas; Popp, Birgit; Bäckström, Tom

Evaluating privacy, security, and trust perceptions in conversational AI: A systematic review

Published in:
Computers in Human Behavior

DOI:
10.1016/j.chb.2024.108344

Published: 01/10/2024

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

Published under the following license:
CC BY-NC-ND

Please cite the original version:
Leschanowsky, A., Rech, S., Popp, B., & Bäckström, T. (2024). Evaluating privacy, security, and trust perceptions in conversational AI: A systematic review. *Computers in Human Behavior*, *159*, Article 108344. https://doi.org/10.1016/j.chb.2024.108344

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Evaluating privacy, security, and trust perceptions in conversational AI: A systematic review

Anna Leschanowsky [a,*], Silas Rech [b], Birgit Popp [a], Tom Bäckström [b]

[a] Fraunhofer IIS, Am Wolfsmantel 33, Erlangen, 91058, Germany
[b] Aalto University, Konemiehentie 1, 02150 Espoo, Finland

ARTICLE INFO

Keywords:
Privacy perception
Security perception
Trust perception
Conversational AI
Systematic review

ABSTRACT

Conversational AI (CAI) systems which encompass voice- and text-based assistants are on the rise and have been largely integrated into people's everyday lives. Despite their widespread adoption, users voice concerns regarding privacy, security and trust in these systems. However, the composition of these perceptions, their impact on technology adoption and usage and the relationship between privacy, security and trust perceptions in the CAI context remain open research challenges. This study contributes to the field by conducting a Systematic Literature Review and offers insights into the current state of research on privacy, security and trust perceptions in the context of CAI systems. The review covers application fields and user groups and sheds light on empirical methods and tools used for assessment. Moreover, it provides insights into the reliability and validity of privacy, security and trust scales, as well as extensively investigating the subconstructs of each item as well as additional concepts which are concurrently collected. We point out that the perceptions of trust, privacy and security overlap based on the subconstructs we identified. While the majority of studies investigate one of these concepts, only a few studies were found exploring privacy, security and trust perceptions jointly. Our research aims to inform on directions to develop and use reliable scales for users' privacy, security and trust perceptions and contribute to the development of trustworthy CAI systems.

1. Introduction

Conversational AI (CAI) systems use AI to enable natural conversations with users via voice or text. Voice-enabled assistants such as Amazon's Alexa or Apple's Siri have gained widespread adoption and can be integrated into devices such as smart speakers or smartphones. At the same time, text-based CAI systems have been on the rise with the increasing usage of chatbots and the emergence of Large Language Models (LLMs) (Vixen Labs, 2023). The integration of CAI systems into Internet of Things (IoT) devices and assisted living technologies further empowers users with seamless control of their devices (Ammari, Kaye, Tsai, & Bentley, 2019). Despite their remarkable capabilities, CAI systems have been criticized for raising significant privacy concerns and associated threats. Criticism ranges from privacy breaches to the constant listening capabilities and intransparent data handling practices (Bolton, Dargahi, Belguith, Al-Rakhami, & Sodhro, 2021; Edu, Such, & Suarez-Tangil, 2021). These concerns, in turn, can reduce trustworthiness in the manufacturer and its devices leading to undesired user experiences or their complete abandonment (Dzindolet, Peterson, Pomranky, Pierce, & Beck, 2003).

To enable user-centric development and useful experiences, understanding users' perceptions of privacy, security and trust concerning CAI is crucial (Panjaitan & Utomo, 2023). As users increasingly engage in interactions with CAI systems, the exchange of personal data has become ubiquitous, necessitating a robust understanding of the factors influencing users' trust. Previous work has emphasized the need for joint investigations of privacy and trust perceptions including domains such as online trading systems (Carlos Roca, José García, & José De La Vega, 2009), electronic commerce (Liu, Marchewka, Lu, & Yu, 2005; Metzger, 2004), online social networks (Zlatolas, Welzer, Hölbl, Hericko, & Kamisalic, 2019), mobile applications (Kitkowska, Karegar, & Wästlund, 2023) and smart home automation (Schomakers, Biermann, & Ziefle, 2021). Yet, the current state of research regarding joint investigations of these constructs in the context of CAI systems remains largely unexplored. Here, we present a systematic review of privacy, security and trust perceptions in CAI.

We argue that trust in these contexts is not only a function of the security measures protecting privacy but also encompasses the perceived intentions, social components and ethical considerations of

[*] Corresponding author.
E-mail addresses: anna.leschanowsky@iis.fraunhofer.de (A. Leschanowsky), silas.rech@aalto.fi (S. Rech), birgit.popp@iis.fraunhofer.de (B. Popp), tom.backstrom@aalto.fi (T. Bäckström).

https://doi.org/10.1016/j.chb.2024.108344
Received 31 December 2023; Received in revised form 10 June 2024; Accepted 12 June 2024
Available online 18 June 2024

Fig. 1. Wordcloud as an illustration of the used terms for researched devices in privacy, security and trust perception papers.

the entities collecting and managing personal information. This can be seen by the influence that trust can have on technology acceptance based on reputation by institutions (Misiolek, Zakaria, & Zhang, 2002). Therefore, trust and privacy perceptions have been explored along with other factors in context such as technology adoption and usage by combining Technology Acceptance Models (TAM) and trust perception models (Ivarsson & Lindwall, 2023; Marangunić & Granić, 2015) or privacy and security factors (Buteau & Lee, 2021; Kowalczuk, 2018). Yet, due to diverse conceptualizations of privacy, security and trust and their contextual dependencies, generalization and evaluation of their impact on other factors present ongoing challenges.

The privacy and security field has long relied on quantitative as well as qualitative research to assess users' perceptions (Distler et al., 2021; Pattnaik, Li, & Nurse, 2023). These methods have also been applied to investigate trust such as interpersonal trust (Mayer, Davis, & Schoorman, 1995; Rotter, 1967) and trust in automation (Hoff & Bashir, 2015; Jian, Bisantz, & Drury, 2000; Lee & See, 2004). While qualitative research is usually characterized by collecting non-numerical data such as interview transcripts, quantitative research focuses on the collection of numerical data for example by using questionnaires. When assessing peoples' perceptions through the use of quantitative surveys, the reliability and validity of scales are crucial. While valid and reliable scales can offer valuable insights into users' perceptions and can confidently inform businesses and policymakers, unreliable ones lack predictive power and generalizability (Colnago, Cranor, Acquisti, & Stanton, 2022). This could have serious consequences for the credibility of privacy and trust research, investment into privacy-preserving measures, enhancement of trustworthiness in design and influence on policy-making. As privacy and trust have been long and extensively studied, well-established scales play a crucial role in quantifying and understanding the nuances of privacy and trust within technology-mediated relationships. At the same time, reuse and adaption of privacy and trust scales have been critically discussed in the literature (Chita-Tegmark, Law, Rabb, & Scheutz, 2021; Colnago et al., 2022; Gross, 2021; Preibusch, 2013), and it remains an open question whether privacy, security and trust scales originally designed for online environments prove reliable and valid in the context of CAI systems. The emergence of CAI-specific usability scales such as the Voice Usability Scale (VUS) or BOT Usability Scale (Borsci et al., 2022; Zwakman, Pal, & Arpnikanondt, 2021), underscore the necessity to explore reliability and validity of currently used privacy, security and trust scales and to assess the need of CAI-specific metrics.

In this work, we conduct a Systematic Literature Review (SLR) to better understand the breadth of research concerning privacy, security and trust perception in the context of CAI systems. In particular, we (1) aim to understand the current state of research concerning the interplay of privacy, security and trust perceptions in the context of CAI and their influence on factors investigated alongside. Moreover, we want to (2) shed light on currently used conceptualizations, measurement methods and tools and their benefits and limitations, in particular how breaches of privacy can erode trust and how users' perceptions of privacy and trust play an essential role in ensuring the adoption and continuous use of conversational AI systems. Finally, we hope to (3) inform future work on conducting reliable and valid privacy and trust research in the context of CAI, and provide future research directions and encourage researchers to critically assess and discuss investigations in this domain.

2. Related work and contributions

Despite previous research on the interplay of privacy, security and trust perceptions, to the best of our knowledge, systematic reviews of research methodologies and constructs related to privacy, security and trust perceptions have not been conducted..

Trust and privacy have long been explored within the context of online environments, e-commerce, online social networks and Conversational AI (Dekkal, Arcand, Prom Tep, Rajaobelina, & Ricard, 2023; Liu et al., 2005; Maqableh, Hmoud, Jaradat, et al., 2021; Taddei & Contena, 2013). These two concepts share similarities, e.g., being essential for human's daily lives, but also differ, for instance, regarding their legislative implementation (Kosa, 2010). Numerous attempts have aimed to formalize both privacy and trust and to conceptualize their influence on people's perception and behavior in technological systems. Yet, the interplay between privacy and trust remains an open question. Results vary with trust being treated as an antecedent to privacy, outcome of privacy or as a moderating variable (Smith, Dinev, & Xu, 2011). For instance, Liu et al. (2005) proposed a Privacy-trust-behavioral intention model for electronic commerce, showing that privacy significantly influenced behavioral intention mediated by trust. In contrast, in the context of online social networks, Taddei and Contena (2013) compared three different models related to the relationship between control, trust, privacy concerns and online self-disclosure and found that a moderating effect between trust and privacy concerns was most explanatory. As privacy and trust are highly subjective and contextual concepts, it is, however, essential to analyze these findings in the context of their research methodology, measurement scales, and participants sample.

In addition to privacy, the role of security perceptions and their relationship to other concepts in the context of CAI is unclear. While the concept of security is distinct from privacy (Smith et al., 2011), a scoping review on human factors in cybersecurity found that despite their focus on security, privacy was one of the most frequently mentioned words across all texts (Rahman, Rohan, Pal, & Kanthamanon, 2021). Moreover, studies suggest that people may not clearly distinguish between privacy and security, pooling these concepts in their perception (Brüggemeier & Lalone, 2022). Research on social network sites proposes combined models suggesting that perceived privacy and security influence continuance intention mediated by trust and satisfaction (Maqableh et al., 2021). On the contrary, the Privacy-trust-behavioral intention model conceptualizes security as one dimension of privacy (Liu et al., 2005). Our literature review addresses both privacy and security aspects to cover the full range of privacy and security research and to provide insights into how these concepts have been investigated in the context of CAI.

Given the complex interplay of privacy, security and trust, and possible differences concerning technological advances, this systematic literature review aims to shed light on previously explored relationships of trust and privacy perceptions in the context of CAI. So far, systematic literature reviews in this domain have focused on conversational assistants or IoT devices more generally without a dedicated focus on users' perceptions (de Barcelos Silva et al., 2020; Pattnaik et al., 2023), on privacy and security aspects of CAI systems (Bolton et al., 2021; Edu et al., 2021; Maccario & Naldi, 2023) or empirical methods and measurement scales used in usable privacy and security research (Distler et al., 2021; Preibusch, 2013; Rohan et al., 2023). Our SLR uniquely contributes to the field by maintaining a specific focus on voice- and text-based CAI systems and the research methodologies employed to

Table 1
Keywords used in the search queries of the SLR on privacy perceptions.

	(Privacy Perception* OR Perception* of Privacy OR Perceived Privacy OR Security Perception* OR Perception* of Security OR Perceived Security)
AND	(Conversational AI OR CAI OR IoT OR Internet of Things OR Voice Assistant* OR Alexa OR Google Assistant OR Siri OR Virtual Assistant* OR Smart Speaker* OR Chatbot*)

Table 2
Keywords used in the search queries of the SLR on trust perceptions.

	(Trust Perception* OR Perception* of Trust OR Perceived Trust OR Trust)
AND	(Conversational AI OR CAI OR IoT OR Internet of Things OR Voice Assistant* OR Alexa OR Google Assistant OR Siri OR Virtual Assistant* OR Smart Speaker* OR Chatbot*)

assess users' privacy, security and trust perceptions. Consequently, we aim to offer an overview of the varied privacy, security and trust aspects investigated in the context of CAI and their interconnectedness.

Thereby, we aim to answer the following research questions:

RQ1 Which methods are used to research privacy, security and trust perceptions for CAI systems?
RQ2 What constructs and sub-constructs are researched?
RQ3 Which and how often are privacy, security and trust perception scales used in research on CAI?
RQ4 To what extent have privacy, security and trust perception scales, used in research on CAI, demonstrated reliability and validity?
RQ5 Are privacy, security and trust perceptions researched in parallel in the context of CAI?
RQ6 Which topics are researched alongside the evaluation of privacy, security and trust perceptions in the context of CAI?

3. Method

We followed the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) method to conduct our systematic literature review on privacy, security and trust perceptions in CAI (Moher, Liberati, Tetzlaff, Altman, & Group, 2009). In total, we conducted two individual SLRs with one on the topic of privacy & security perceptions and one on trust perceptions in CAI systems. The procedures are outlined in this section and shown in Fig. 2. We first identified relevant research papers before selecting them based on exclusion and inclusion criteria. Afterwards, we assessed their eligibility and selected appropriate records for the final study.

3.1. Search strategy

We included research papers from five databases, i.e. ACM Digital Library, IEEE Xplore, Scopus, Web of Science and SpringerLink. Tables 1 and 2 show the keywords used for searching for records on privacy & security perceptions and trust. While the first subset of keywords captures the aspect of privacy & security or trust, the second subset of keywords covers a variety of words used to describe text-based as well as voice-based Conversational AI systems. As CAI systems are often integrated into Internet of Things (IoT) devices, e.g. smart speakers, smart fridges or smart vacuum cleaners, we included keywords related to IoT in our search query. Similarly to Pattnaik et al. (2023), we included ACM Digital Library and IEEE Xplore as search databases as they are important publishers in the field of privacy and security and smart appliances as well as human–computer interaction. Moreover, we included Elsevier's Scopus and Web of Science as they were shown to be comprehensive yet limited in their overlap (Bar-Ilan, 2018). Finally, we included SpringerLink as a journal platform (Gusenbauer & Haddaway, 2020) for their coverage of psychological journals. We restricted our keyword search to abstracts and included only articles and conference papers.

3.2. Study selection

By following the PRISMA method, we established exclusion and inclusion criteria to select relevant papers. Exclusion criteria were as follows:

- Non-English papers
- Workshop descriptions or book chapters
- Review papers
- Papers that do not cover CAI, e.g. connected cars, smartphone applications, smart meters, blockchain, cryptography, supply chain
- Papers that do not include a user study related to privacy, security or trust perceptions

After excluding papers based on the criteria described above, we included papers assessing privacy, security and trust perceptions in the context of Conversational AI systems. Finally, we conducted backwards and forward snowballing to identify additional relevant papers using ResearchRabbit.[1] We applied the same inclusion and exclusion criteria and stopped snowballing after one iteration.

3.3. Analysis procedure

We developed a data chart to extract relevant variables from the research papers. In addition to more general information such as the date of publication, author's affiliation and publication venue, we focused on more specific attributes related to our research questions. To gain insight into the current landscape of research methods used in the context of privacy and trust perceptions in CAI, we focused on methodological data, e.g. research method, research platform, number, type and location of research subjects. Moreover, we were interested in the response variables that were assessed by the researchers, the quality measures used to ensure reliability and validity and the techniques applied for analyzing the data. We were particularly interested in the variety of response variables that were evaluated within one study as well as their origins.

4. Application fields and devices, research methods

4.1. Selected papers

Our paper selection process is shown in Fig. 2. Our final selection resulted in 100 papers related to privacy and security perceptions and 58 papers on trust perceptions. While IoT was found a useful keyword in combination with security and privacy perceptions, it led to the exclusion of a majority of papers in combination with trust perceptions. Here, trust in the context of IoT is mostly concerned with zero-trust policies between devices rather than the assessment of trust perceptions with a human counterpart in the interaction with a CAI system. Despite previous research in other domains on the interplay of privacy and trust, surprisingly, we identified only three papers that were found by both literature searches (Lappeman, Marlie, Johnson, & Poggenpoel, 2023; Pal, Babakerkhell and Roy, 2022; Seymour, 2023). We will discuss this finding in more detail in upcoming sections.

4.2. Time trend

Fig. 3 shows the yearly trend of selected papers for privacy, security and trust. Although we did not restrict our search to a specific timeline, the first papers in our final selection were found in the year 2015 for literature on privacy and security and in the year 2018 for trust. The appearance, as well as the time trend, is in line with previous literature research on privacy in smart speakers (Maccario & Naldi, 2023) and

[1] https://www.researchrabbit.ai/.

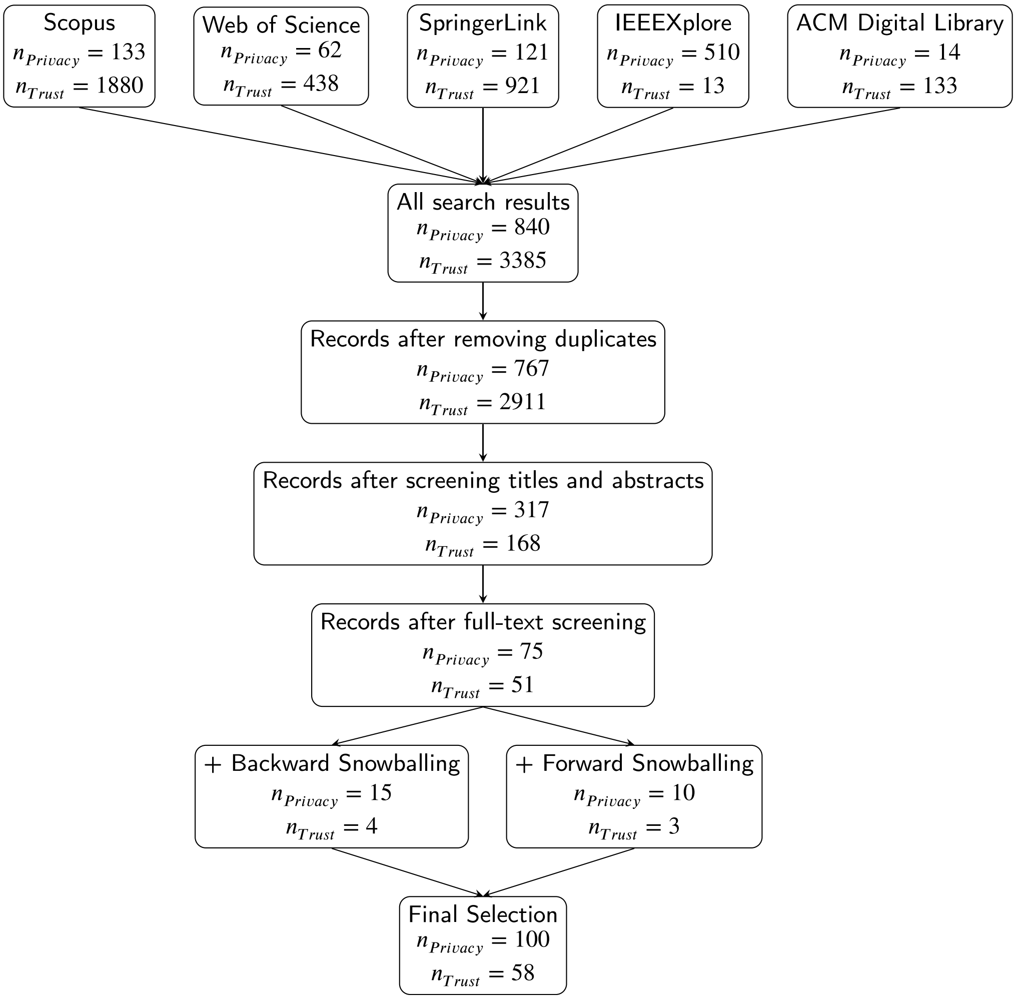

Fig. 2. PRISMA procedure used for the systematic literature review on privacy, security and trust perceptions.

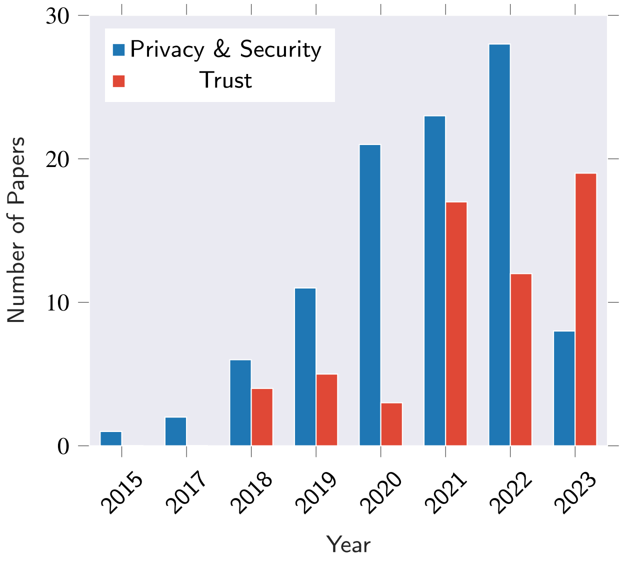

Fig. 3. Number of papers over time with the most recent paper from June 2023.

on home networking environments (Pattnaik et al., 2023). Although Apple's Siri was already released in 2011 followed by Amazon's Alexa in 2014, media coverage on privacy concerns around these devices experienced a strong increase with Amazon handing over recordings to investigators[2] and increasing awareness about workers listening in on customer's conversations.[3] We chose June 2023 as the cut-off for our systematic search. The actual number of papers published on both topics is expected to be higher for all of 2023 which supports the increasing trend of research in this field. The most recent paper was added by snowballing in November 2023.

4.3. Geographical distribution

Fig. 4 shows the author's affiliation by country for each of the constructs. It is not surprising that the majority of authors are affiliated with a US institution (27%) followed by the UK (13%) and Germany (9%) for privacy & security. Similar results were shown by Maccario and Naldi (2023) when surveying privacy research for smart speakers. The results show that the headquarters of large CAI manufacturers, such as Amazon, Google or Apple are not directly linked to the author's affiliation by country.

A similar phenomenon can be observed for trust in CAI where the US leads with 13.75%, China (11.25%) and Germany (10%). We find that there is a significant difference between countries researching privacy and trust in terms of the number of publications and global diversification. In particular, the numbers suggest that the political system

[2] https://www.bbc.com/news/technology-39191056.

[3] https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio.

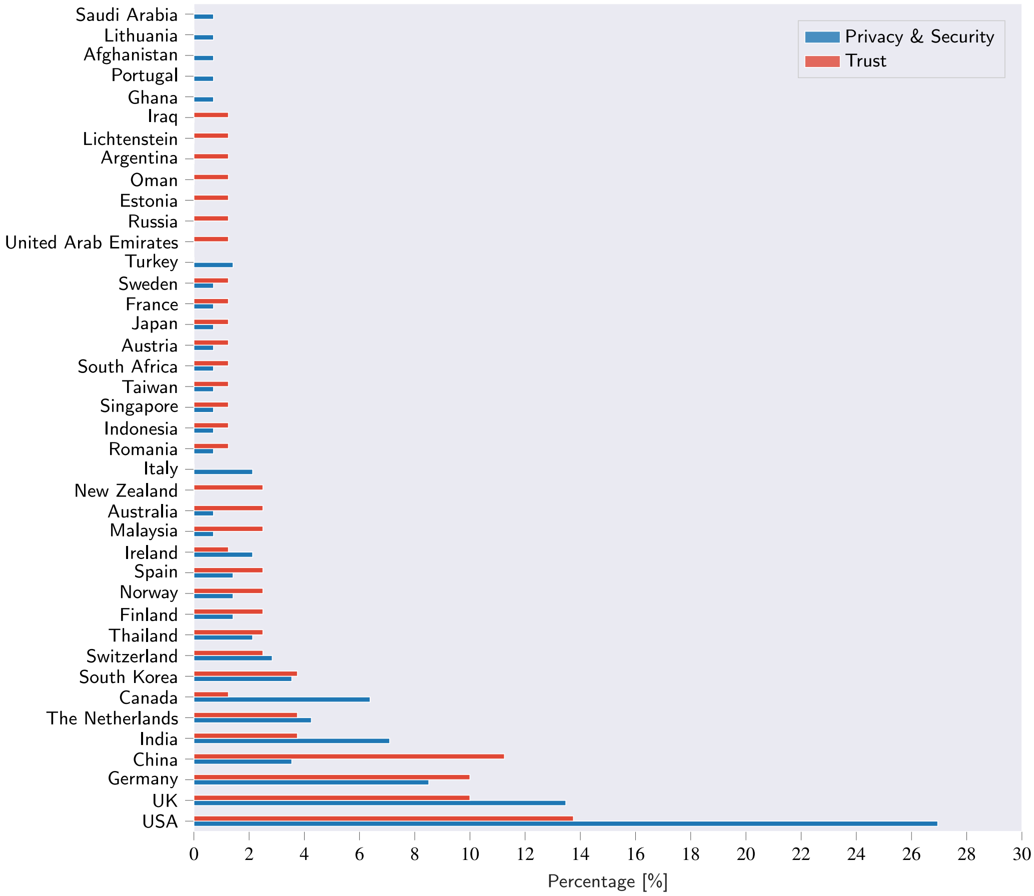

Fig. 4. Author's affiliation by country for privacy, security and trust perception papers in percentage. Due to the different number of papers for Privacy & Security and Trust, papers can have multiple authors from varying countries.

and possibly associated status of privacy influence whether research is conducted on privacy or trust perceptions. Another reason could be that trust is a more generic term contrary to privacy and security and its dominance across several research fields influences publication counts per country. Moreover, the concept of trust positively impacts technology adoption (Choung, David, & Ross, 2023), while privacy and security are often seen as inhibitors to adoption and innovation which could be another reason for researchers to focus on one or the other. It needs to be mentioned that the research communities vary greatly on a per-country basis, thus the number of reported papers is not representative of the overall research output from a particular country. Additionally, we are aware that reporting the overall research output per country does not consider the research capacity each country has based on the number of researchers in each country. Thus, we cannot draw any conclusions on how relevant "privacy & security" and "trust" research in each country is. However, it allows a comparison between the research communities of "privacy & security" and "trust" perceptions.

4.4. Devices and modalities

In our literature review, we focus on Conversational AI systems – systems that leverage natural language processing capabilities to converse with humans. Thereby, we include text-based as well as voice-based systems. While we aimed to cover the most prevalent terms for CAI systems in our keyword search, a detailed analysis of the devices researched by the identified papers shows the diversity of terms used to describe CAI systems. Fig. 1 shows a word cloud of researched devices as described by the authors of the paper in their titles or abstracts. In combination with privacy and security perceptions, the word "smart speakers" was used most (15%) when describing researched devices, followed by "voice assistants" (10%) and "IoT devices" (6%) and "Intelligent Personal Assistants" (6%). In particular, we find that all studies on "IoT devices" include smart speakers as researched devices in addition to other IoT devices (Ahmad, Farzan, Kapadia, & Lee, 2020; Al-Ameen, Chauhan, Ahsan, & Kocabas, 2021; Alghamdi, Alsoubai, Akter, Alghamdi, & Wisniewski, 2022). Thus, increasing the number of studies that research "smart speakers" to 21%. In the context of trust perceptions, the word "assistant" is most frequently used with 41%, either in combination with "virtual"(48%) or "voice"(52%). This is followed by "chatbots" as research devices with 22% and then by "Alexa"as a research device (12%).

We further categorize the researched devices depending on their modality. We find that a majority of privacy and security-related papers focus on voice as a modality (76%), while 16% focus on text as the main modality. Thereby, all of the studies researching privacy perceptions in text-based CAI systems refer to their systems as "bot" or "chatbot" (Cheng & Jiang, 2020; Patil & Kulkarni, 2022; Van Der Goot & Pilgrim, 2020). Yet, some acknowledge that chatbot can be used as a more general term including text as well as voice-based conversations. The remaining papers do not explicitly specify the modality or refer to their researched devices more generally as "virtual assistants" or "agents". Similarly, in trust research 50% of papers conduct research on voice-based systems. 36% focus on primarily text-based systems, which are exclusively called chatbots just as in privacy research. Additionally, in trust papers, we identified 14% of papers as virtual reality-related. Since all papers on virtual reality use voice as a mode, the total percentage of voice-based systems increases to 64%.

Table 3
Application fields for privacy & security and trust perception in the context of CAI. Application fields were identified via keywords, titles and abstracts.

Application field	Privacy & security - Frequency (Percentage)	Trust - Frequency (Percentage)
General	58 (58%)	37 (64%)
Smart home	15 (15%)	4 (7%)
Healthcare	6 (6%)	2 (3%)
Retail	5 (5%)	5 (9%)
Finance	5 (5%)	3 (5%)
Customer service	5 (5%)	2 (3%)
Education	3 (3%)	2 (3%)
Workplace	1 (1%)	–
Insurance	1 (1%)	–
Hospitality	1 (1%)	–
VR	–	3 (5%)
Space flight	–	2 (3%)
Self driving	–	1 (2%)

Table 4
Research methods in our sample.

Research method	Privacy & security - Frequency (Percentage)	Trust - Frequency (Percentage)
Quantitative	60 (60%)	47 (81%)
Survey	45 (45%)	22 (38%)
Experiment and survey	12 (12%)	11 (19%)
Vignette study	3 (4%)	14 (24%)
Trust game	–	2 (3%)
Mixed	19 (19%)	6 (10%)
Qualitative	21 (21%)	5 (9%)

4.5. Application fields

Table 3 shows the application fields targeted by the reviewed studies. To identify application fields, we relied on keywords, titles and abstracts. We refer to "General" whenever an application field is not explicitly mentioned. For privacy & security perceptions, 58% did not target a specific application field. A similar trend can be observed in the context of trust perceptions. Nevertheless, additional application fields such as virtual reality (VR) or space flight were identified. This finding leaves room for future research to explore privacy, security and trust perceptions of CAI systems targeted towards under-researched applications. In particular, it might be valuable to explore fields that have been researched in the context of trust perceptions but not privacy and security perceptions and vice versa to better understand their interplay and contextual dependencies. Moreover, only a few papers target more than one application field or compare privacy, security and trust perceptions among them. For example, Brüggemeier and Lalone (2022) investigate conversational privacy across three different application areas, i.e. banking, tax advice and music control.

4.6. Research methods

One of the goals of our literature review was to identify common research methods used to study privacy, security and trust perceptions in CAI. We show an overview of research methods used by the analyzed papers in Table 4. A more detailed overview is provided in the Appendix in Table 18. To classify the study methods, we relied on previous classification schemes used to review empirical methods in usable privacy and security research (Distler et al., 2021). Therefore, we refer to *experiments* whenever the effect of experimental conditions was measured either through oral examination or written questionnaire form. We further distinguish between *survey studies* that use written questionnaires to interrogate people and *interview studies* with an oral interaction between the researcher and participants. We coded qualitative methods that included a survey to identify participants, e.g. smart speaker users, as qualitative methods only because the surveys served only the purpose of identification and were usually not analyzed further. Finally, we explicitly coded less common study methods and combinations of those, e.g. focus groups, co-design methods or trust games. Trust games originate, among others, from the investment game introduced by Berg, Dickhaut, and McCabe (1995) to measure trust in economic settings. In this paradigm, one participant allocates funds to a different location, where a second participant deliberates on whether and to what extent to reciprocate the amount to the first participant. The underlying objective is to directly gauge levels of trust and the willingness to undertake risks for the prospect of a favorable outcome.

We found that in both cases, i.e., privacy & security and trust perceptions, a majority of analyzed papers used quantitative methods. While quantitative methods can be used to test hypotheses, qualitative methods can provide rich, detailed data that helps in understanding the complexity of a particular issue and can be used to form hypotheses (Lazar, Feng, & Hochheiser, 2017). Thus, diversification of research methods is generally desirable as both methods complement each other and help to advance the research field.

Interestingly, we identified a significant difference in the number of papers using qualitative and mixed research methods to assess privacy and trust perceptions. While 21% and 19% respectively applied qualitative or mixed methods to assess privacy and security perceptions, only 10% of trust papers were qualitative, and only 9% were mixed methods. For research on trust perceptions, questionnaires were identified as the most common form of measurement possibly due to the difficulty of measuring trust indirectly from other sources such as bio-signals or other behavior tracking (Bauer & Freitag, 2018). In the context of privacy and security perceptions, mixed study methods including multiple different methods are common. For example, Kowalczuk (2018) analyzed customer reviews and Twitter data to identify factors influencing smart speaker usage intentions before evaluating the acceptance model through a user study. In another study, Malkin et al. (2019) applied experience sampling methodology to expose participants to their past smart speaker interactions followed by privacy perception and preference assessment. In contrast, research on trust perceptions applied less diverse study methods in mixed-method settings and relied predominantly on *mixed surveys* that contained additional open-ended questions in the survey which were investigated qualitatively (Nordheim, Følstad, & Bjørkli, 2019).

Our sample showed a predominance of survey methods which is in line with Distler et al. (2021). While their review focused on usable privacy and security research, they showed that research on privacy and security perceptions, attitudes and behavior was dominated by descriptive studies. These studies were also less likely to include prototypes and relied heavily on self-reports. We agree with Distler et al. (2021) that methods that have not been deployed frequently could not only help advance the usable privacy and security research field but help to gather more diverse insights on privacy, security and trust perceptions. For example, long-term perceptions of privacy and trust can be assessed via diary studies – a research method that has been rarely used in our reviewed sample. Moreover, triangulation of various methods can deepen insights and help to understand results (Pettersson, Lachner, Frison, Riener, & Butz, 2018), for instance, by combining interviews and analysis of log files (Ammari et al., 2019). Here, research on trust perceptions could rely on mixed-method studies already applied in the field of privacy and security. Finally, the usage of prototypes can also enhance studies on privacy and trust perceptions by making scenario-based situations more concrete (Distler et al., 2021). We will discuss tools in more depth in Section 5.5.

4.7. Recruitment methods

We further analyzed recruitment strategies addressed by our sampled papers to enhance our understanding of target groups as shown in Table 5. Thereby, we listed all used recruitment methods for each study

Table 5
Recruitment methods for participants used in the analyzed papers. Papers can use multiple recruitment methods.

Recruitment method	Privacy & security - Frequency (Percentage)	Trust - Frequency (Percentage)
Crowdsourcing	38 (29%)	23 (32%)
Internet and social media	27 (21%)	9 (14%)
University	23 (17%)	8 (11%)
Not reported	16 (12%)	23 (32%)
Personal network	14 (11%)	7 (10%)
Special facilities	9 (7%)	–
Paper advertisement	4 (3%)	1 (1%)

Table 6
Type of participants researched in the analyzed papers. Papers can use multiple different types. Participants can be part of more than one category.

Type of participants	Privacy & security - Frequency (Percentage)	Trust - Frequency (Percentage)
Technology users	48 (32%)	2 (3%)
Crowd workers	37 (26%)	31 (50%)
Students	17 (12%)	18 (29%)
Special user group	15 (10%)	–
Not reported	11 (7%)	7 (11%)
Experts	9 (6%)	4 (7%)
Non-users	6 (4%)	–
Employees	5 (3%)	–

as it was not uncommon that multiple methods were applied. As privacy, security and trust perceptions are highly subjective, recruitment strategies are crucial to identify to what extent study results are generalizable. As an easily accessible recruitment method, it is not surprising that crowdsourcing has been applied most frequently using platforms such as Amazon Mechanical Turk, Qualtrics or marketing research agencies. Social media and online platforms, including blogs and social networks, also featured prominently, while traditional methods such as paper advertisements were notably infrequent and often only used in the context of recruitment of older adults. Interestingly, some of the analyzed papers investigating privacy and security perceptions relied on special facilities to recruit specific target groups such as patients or seniors while analyzed papers on trust perceptions did not.

Crowdsourcing predominated in quantitative studies, while qualitative and mixed-method studies leaned towards personal networks, paper advertisements, and university channels. This was also confirmed by the difference in average participant numbers, with quantitative studies totaling an average of 427 and 273 participants, in privacy & security and trust research respectively compared to the 26 to 29 participants in qualitative studies. It is noteworthy, that the lowest quantitative study found in the context of trust perceptions has 13 participants which is lower than the average number of participants in the qualitative studies (Gupta et al., 2019).

4.8. Participants

As shown in Table 6, we grouped participants into more specific groups. It needs to be noted that participants can be part of more than one category, e.g., they might have been students or crowd workers as well as technology users. We find that a majority of papers evaluating privacy and security perceptions specifically recruited technology users for their studies while research on trust perceptions did not. Frequently, crowd workers were screened for their technology usage before participation in the study. For trust, a more general type of participants is desired as can be seen by the majority of participants in trust research being crowd workers. Overall, students form another significant research group and are generally a result of convenience sampling. Special user groups encompass patients, older adults or visitors of smart homes while the group of experts consists of developers, medical professionals as well as teachers. Finally, a few studies in the domain of privacy and security perceptions, recruited employees including university staff, forming a convenience sample (Fahn & Riener, 2021; Hornung & Smolnik, 2022; Liao, Vitak, Kumar, Zimmer, & Kritikos, 2019; Mols, Wang, & Pridmore, 2022).

5. Measurements of privacy, security and trust perceptions

Next to comparing meta-information of the studies, like author affiliations, participants, researched devices and application fields in privacy, security and trust research, we investigate the developed and used privacy, security and trust perception measurements in the reviewed papers.

5.1. Qualitative privacy, security and trust assessment

The assessment of qualitative studies was conducted by grouping their findings. Within the qualitative trust literature, there were no papers that defined response variables, or trust-related questions used in the interviews. Instead, relevant items were identified after the interviews were conducted with audio recordings, transcriptions or field notes among others. Across all papers that used a qualitative approach, we could not identify any overlapping theme or item used across papers but the perception of giving up privacy when using voice assistants (Fakhimi, Garry, & Biggemann, 2023; Perez Garcia & Saffon Lopez, 2018). Perez Garcia and Saffon Lopez (2018) also note a questionnaire with 500 hundred individuals. However, there is neither a statistical analysis of the questionnaire nor discussion of individual items.

Further, the benefits of interactions, in terms of utilitarian, hedonic and social aspects, were included in Fakhimi et al. (2023) which emphasize the more social influence of trust in interactions. Similarly, the effect of anthropomorphized voice assistants was subject to the interviews of this paper. Next to anthropomorphized analysis stands a design approach that was taken in Durall Gazulla, Martins, and Fernández-Ferrer (2023). The differences between research approaches make the comparison and analysis of qualitative papers challenging.

Due to the large differences in researched items within the qualitative studies, as well as in comparison to the quantitative approach, we did not include the qualitative findings further into the literature review of this study.

5.2. Quantitative privacy, security and trust assessment

Next, we aim to understand how privacy, security and trust perceptions are quantitatively measured in the context of CAI and which constructs are assessed.

5.2.1. Privacy, security and trust scales and constructs

We analyze the privacy, security and trust scales used to assess peoples' perceptions in quantitative and mixed-method studies. Table 7 provides an overview of constructs assessed by studies evaluating privacy, security and trust perceptions. We extracted response variables from the detailed questionnaires that were published by a majority of papers. It is noteworthy that in general more than 80% of papers reported on the detailed items and questions assessed in the surveys. Nevertheless, with the remaining papers not reporting on used scales, there is still room for improving transparency and reproducibility for the privacy and trust research community. We extracted response variables from the published research models, survey and results sections for this subset. Moreover, we found that detailed scales were often referenced from the source neglecting adaptations made by the authors and hindering reuse and replicability of scales. We can see 56 of all papers referencing trust as a construct in their work which is followed by 40 papers referencing privacy concerns directly. Further, we distinguished between trust and trust & technology constructs to highlight the difference between scales used in the CAI context. As CAI systems are technical systems, it is concerning that only a minority of papers use trust scales developed for the technological context.

Table 7
Overview of privacy, security and trust constructs used in mixed-method and quantitative studies. Studies can assess multiple constructs. A detailed overview is provided in Appendix Tables 16 and 17.

Construct	Frequency
Trust	55
Privacy concerns	40
Affect, humanness and anthropomorphism	29
Risk perception	29
Character and personality	14
Security and security perception	11
Control	8
Trust & technology	11
Privacy and privacy perception	4
Interactivity	3

Privacy and privacy perception. We find that the reviewed literature explores diverse privacy and privacy perception constructs. As no generally agreed-upon definition of privacy exists, studies must be as explicit and detailed about their privacy conceptualizations and measures as possible to allow traceability and reproducibility. For example, in the study by Furini, Mirri, Montangero, and Prandi (2020) participants are asked about the importance they attribute to privacy and their willingness to use a service capable of surveillance in particular in the context of violating COVID-19 lockdown measures. However, neither in their questionnaire nor in the paper, do they provide a definition or explanation of privacy. Conversely, Krey and Ramirez Garcia (2022) focus on unique characteristics of voice assistants to assess privacy by asking hospital patients about their privacy concerns related to the passive-listening capabilities of the device, the necessity of providing information about privacy risks and concerns around the voice assistants disclosing patient's personal information loudly. Based on these three questions, privacy is narrowly defined within the study context, yet, comparability to established privacy conceptualizations is limited (Smith et al., 2011). Similarly, Patil and Kulkarni (2022) do not define privacy but rely on a previously used privacy scale including questions on disclosure, the importance of regulations and trustworthiness. In contrast, Brüggemeier and Lalone (2022) investigate conversational privacy and provide a conceptualization by drawing from previous literature. Thus, they refer to conversational privacy whenever CAI systems "express privacy-related information in dialogue form" (Brüggemeier & Lalone, 2022; Harkous, Fawaz, Shin, & Aberer, 2016; Lau, Zimmerman, & Schaub, 2018).

Control. Six studies specifically investigate privacy control, perceived control, controllability and privacy boundary control (Ahmad et al., 2022; Alghamdi et al., 2022; Kang & Oh, 2023; Lin & Parkin, 2020; Pal, Arpnikanondt, & Razzaque, 2020; Purwanto, Kuswandi, & Fatmah, 2020). Alghamdi et al. (2022) and Pal et al. (2020) conceptualize control as "users' ability to control their personal information". Importantly, they focus on control over existing as well as future generated data (Pal et al., 2020). Lin and Parkin (2020) investigated perceptions of control and compared privacy control usage relying on existing privacy controls such as voice authentication or muting and unplugging of devices. Finally, Kang and Oh (2023) draw from Communication Privacy Management (CPM) theory and conceptualize boundary control as "users' control over the process of withdrawing and controlling personal information". While the aforementioned studies conceptualize control as control over personal information, Purwanto et al. (2020) describes controllability as one facet of interactivity and as a general feature that allows users to manipulate the interaction, e.g. content and timing, with a digital assistant.

As studies keep investigating privacy control, it is necessary to state what is being controlled and which dimensions of control are considered. For instance, Brandimarte, Acquisti, and Loewenstein argue that one needs to distinguish between control regarding the release of personal information, access to it as well as further usage. While people may be most likely to focus on control regarding the disclosure of personal information, control over access and usage might be more relevant to their privacy. Despite the limited exploration of privacy as control in the context of CAI systems in our sample, the studies that do exist, assess control indeed across various dimensions. While two studies focus on control over the collection of personal information and its influence on disclosure, Lin and Parkin (2020) provides a detailed analysis of privacy controls encompassing control over data access and data retention.

The majority of studies investigating privacy control in our sample refer to a common conceptualization of privacy, i.e., users' ability to control their information (Smith et al., 2011). However, scholars have argued that control should not serve as a proxy for privacy as privacy situations can exist without someone perceiving or exercising control (Laufer & Wolfe, 1977). For instance, choosing privacy-preserving technology in the first place reduces the need to control information during usage. Thus, individuals might not perceive control at the time of usage while still perceiving a high level of privacy. In addition, what matters to privacy is the amount of information others have access to and the appropriateness of the flow of information (Nissenbaum, 2009). This can be seen as independent of whether an individual controls the information flow or someone else, e.g., data protection authorities monitor the application and if necessary apply corrective measures.

The above discussion necessitates a detailed and explicit description of constructs and methodological transparency when assessing privacy control.

Privacy concerns. The predominantly assessed construct in the context of privacy is privacy concerns. While most studies assess privacy concerns more generally, Lutz and Newlands (2021) evaluate seven distinct types of privacy concerns among smart speaker users. Their findings reveal that institutional actors such as third-party companies lead to stronger privacy concerns compared to social actors such as household members. Along the same lines, Pal, Babakerkhell et al. (2022) investigate the impact of various types of privacy concerns on trust and usage of voice-activated personal assistants. They find that privacy concerns related to the voice assistants and the household have a significant impact on users' emotional and cognitive trust. However, vendor and third-party privacy concerns only significantly affect emotional trust while government privacy concerns have no significant effect. While most reviewed papers investigate general privacy concerns, the previously discussed studies suggest various dimensions of privacy concerns should be considered. In particular, distinctions between horizontal or social and vertical or institutional privacy concerns could be beneficial to enhance understanding of the influence of privacy concerns on trust and in specific contexts, e.g., public domain or multi-user context (Ayalon & Toch, 2019; Masur, 2019).

Security and security perception. In addition to exploring privacy perceptions, investigations into security and security perceptions in the context of CAI systems have been conducted. It is crucial to recognize that privacy and security are distinct concepts. While security is considered a necessity for privacy, security does not necessarily hinder subsequent usage of personal information, potentially leading to privacy breaches (Ackerman, 2004; Culnan & Williams, 2009). While various definition of security exists, it commonly refers to the protection of personal information concerning integrity, authentication, and confidentiality (Smith et al., 2011). Therefore, it comes as no surprise that security perceptions in our identified studies have been assessed in the context of attack susceptibility of voice assistants (Krey & Ramirez Garcia, 2022; McCarthy, Gaster, & Legg, 2020), or authentication methods (Renz, Neff, Baldauf, & Maier, 2023), and in contexts with heightened sensitivity such as banking (Brüggemeier & Lalone, 2022; Fahn & Riener, 2021), shopping (Aw, Tan, Cham, Raman, & Ooi, 2022) or device sharing scenarios (Lee, Kim, & Choi, 2019). Furthermore, most studies assessed security perceptions alongside privacy perceptions or privacy concerns while acknowledging the differences between these concepts. For instance, Buteau and Lee (2021) define privacy concerns according to Dinev and Hart (2005) as "perceived vulnerability and ability to control ones' information" while they refer to perceived security as "perceptions regarding reliability of mechanisms of data transmission and storage" according to Flavián and Guinalíu (2006). Their results show that privacy concerns negatively influence attitudes towards using voice assistants while security perceptions contribute positively. They particularly highlight participants' distinct understanding of privacy and security as separate concepts. Another study investigated the effect of conversational privacy on both privacy and security perceptions in three distinct contexts, i.e., banking, tax and music (Brüggemeier & Lalone, 2022). While they found that conversational privacy can positively impact privacy and security perceptions, no significant differences between privacy and security perceptions were reported. This shows that the type of privacy construct studied alongside security perceptions influences the understanding of the complex relationship between privacy and security perceptions in CAI systems.

Risk perception. As shown in Table 7 risk perceptions are frequently mentioned, in total 29 times. Notably, the majority of papers assess risk perception in the context of structural models that aim to evaluate factors impacting CAI adoption, usage and more. Many of these studies build upon the Technology Adoption Model (TAM) or related conceptual models and extend them by adding factors like perceived privacy risk, perceived security risk, or safety risk. For instance, Kowalczuk (2018) evaluated security and privacy risks as a combined construct conceptualizing them as consumers' fears of personal information leakage or hacking. Similarly, Han and Yang (2018) jointly assess security and privacy risks but using only a subsection of an established scale. We will discuss extensions of technology adoption models that include risk perception in more detail in Section 5.3.

In our sample, only few papers independently discussed risks. Nordheim et al. (2019) investigated factors including risks that influence trust in customer service chatbots. Based on previous literature, they conceptualize risk as "Users' perceptions regarding the likelihood of an undesirable outcome". Their findings show that perceived risk significantly influences users' trust in chatbots. In another study, focused on privacy and security labels for smart devices, including smart speakers, Emami-Naeini, Dheenadhayalan, Agarwal, and Cranor (2021) assessed participants' risk perception of label attribute–value pairs, e.g. security update - automatic. They found that the risk perception was influenced by the displayed label pairs, effectively conveying information. Song, Du, Xing and Mou (2022) conduct a scenario-based experiment investigating the self-recovery approaches of chatbots on consumer satisfaction while considering perceived privacy risks. They identified a moderating role of robot intelligence on perceived privacy risks in chatbot self-recovery.

The variation in risk perceptions observed in our sample mirrors the fragmented notion of privacy perceptions. Moreover, none of the identified studies distinguishes dimensions of risks nor risks, consequences and sources (Lim, 2003). Given the various application areas of CAI, future research should investigate more fine-grained risk perceptions. Additionally, on a conceptual level privacy perceptions, privacy concerns and privacy risks are distinctively different from privacy risks relating to an individual's perception of risks in a specific state. In contrast, privacy concerns should generally be treated as a trait-like characteristic (Smith et al., 2011). Therefore, when evaluating systems or designs concerning privacy, it is advisable to assess perceived privacy risks, while privacy concerns are neglectable.

Trust. Trust was the most assessed construct in the reviewed literature, with a total of 56 papers. However, it needs to be pointed out that using the overall term "trust" can be misleading since the definition of trust largely differs on a per-paper basis. Some just define trust as how safe a mobile payment is and how little it will hurt privacy (Jameel & Karem, 2022) while others include brand trust and emotional components as in Lappeman et al. (2023). Others define trust as "the belief that an entity will act cooperatively to fulfill clients' expectations without exploiting their vulnerabilities" (Seymour, 2023). Further, trust is broken down into sub-constructs, such as competence, which is already built-in in the model of Mayer et al. (1995). This can lead to confusion when trust is measured as a single item, or as competence like in Pesonen (2021).

Trust models consists of items, which directly ask the participants about their trust perception for which an interpersonal scale is often used, as the machine-part is seen as another person. Hence, there is no difference between human–human and human–machine communication (Weidmüller, 2022). Weidmüller (2022) includes human-like and machine-like trustworthiness as items. Further, trust items can be investigated more specifically. Lappeman et al. (2023) include brand trust in their questionnaire design as a relevant factor for overall trust levels in the interaction. On the other hand, Jiang, Yang, and Zheng (2023) include task-specific trust in their work as a component, since there is the assumption that one might show trust to a person well-qualified for a task. However, this does not guarantee that the same person will be given the same trust during a different task.

Trust (Mayer). The Mayer model of trust is highly accepted in trust measurement such that a multitude of papers used items directly from that scale. Therefore, items like integrity, benevolence, competence, technical competence, perceived benefits and reputation are all included in the trust scales. This subgroup emphasizes the influence that the trust model of Mayer has on the development of trust scales over the last years. It raises the question of to what degree the Mayer model should be used in trust in technology context – particularly in the context of CAI – since the original model has an organizational, interpersonal focus.

Trust and technology. A larger subgroup of trust can be trust and technology, which all contain items relevant to technology. Following the origins of the constructs used in the studies revealed that there were only two scales used. First, the scale by Jian et al. (2000) was developed in 2000 – a time when neither AI nor Chatbots were as sophisticated as today – and second, the scale by Gupta et al. (2019) marks one of the most recent development steps of a human–computer trust scale within the last years. Yet, for the latter one, it needs to be mentioned that three items (benevolence, competence and perceived risk) stem from the Mayer model. Further, we found the scale developed by Jian et al. (2000) being mentioned in both, trust in automation and trust scales. This leads to confusion as the context in which the scale was developed matters.

Interactivity. A smaller subgroup, namely three papers use interactivity as one of the constructs in their scales (Hu, Lu, et al., 2021; Prakash, Joshi, Nim, & Das, 2023; Purwanto et al., 2020). This is surprising, especially when considering that interactiveness is essential in the perception of a human-like interaction between a CAI system and a human. The trust research community could benefit from an additional focus on interactivity, especially in the context of CAI systems.

Affect, humanness, anthropomorphism. A crucial and often overlooked aspect of trust, next to task-solving capabilities, is the integration of affect reaction in CAI systems. We cluster perception of humanness by assistants as one group which contains items like social presence, which is often used in technology acceptance studies, humanlikeness (Lv, Hu, Liu, & Qi, 2022), understanding humanness (Hu et al., 2021) or anthropomorphism (Chen & Park, 2021). Interestingly, perceived humanity, perceived social presence and perceived social interactivity are originally part of a technology acceptance study (Venkatesh & Davis, 2000). Items like faith and personal attachment stem from the development of a human–computer trust scale (Madsen & Gregor, 2000), but they were only used in one study (Lee & Sun, 2022).

Character and personality. Next to items directly related to trust, another group of items identified in a variety of papers was items related to character and personality. Already Mayer et al. (1995) identified that to some degree depends on the 'propensity to trust' which is highly personality dependent. This indicates that there might be other factors related to character and personality, that could be relevant for trust measures. Müller, Mattke, Maier, Weitzel, and Graser (2019) integrated a complete personality questionnaire into their study to see what effect personality has on trust measures and development. This was further supported by items like self-esteem or disposition to trust.

5.2.2. Scale development and reuse

After discussing which constructs have been researched to assess users' privacy, security and trust perceptions, we were further interested in which scales were used or referred to in detail (RQ3). Therefore, we analyzed the extent to which studies developed or reused scales to investigate privacy, security and trust perceptions.

We find that research on trust perceptions largely reuses and adapts scales %removedrather than developing their own. Similar observations were made for privacy and security scales with more than 80% of papers relying on scales used in prior work. Whenever scales were not explicitly reused or adapted from previous work, researchers mostly used single items or multiple distinct questions. For example, Gauder et al. (2023) and Tenhundfeld, Barr, Emily, and Weger (2021) use a single item to evaluate confidence and trust. Similarly, Joy, Kotevska, and Al-Masri (2022) rely on a single question to measure participants' level of data privacy concerns. Yet, such single-question instruments are rarely developed methodologically and lack reliability and consistency measures (Preibusch, 2013).

We were further interested in whether specific scales dominated the assessment of privacy, security and trust perception research in the context of CAI. While Jian et al. (2000) and Lankton, McKnight, and Tripp (2015) were frequently cited as a source and origin for trust in technology in Table 17(Appendix), the same does not hold for privacy and security perception measures. This is surprising as, despite the existence of established scales for measuring privacy concerns (Preibusch, 2013), only a few papers report references to these scales.

Only three studies specifically cite the well-known privacy concern scale (CFIP) (Park, Choi, & Jung, 2021; Smith, Milberg, & Burke, 1996; Uysal, Alavi, & Bezençon, 2022; Vimalkumar, Sharma, Singh, & Dwivedi, 2021). However, while the original CFIP scale consists of four sub-scales related to collection, errors, unauthorized secondary use and improper access, Uysal et al. (2022) utilized only one subscale, consisting of four items, to evaluate privacy concerns. Similarly, Cho, Sundar, Abdullah, and Motalebi (2020) rely on a scale originally designed with thirteen items to measure privacy concerns but uses only three. In general, altering well-established scales should be done with caution as it may invalidate existing reliability and validity (Preibusch, 2013). Nevertheless, using well-established scales in new contexts such as CAI systems, could help in reevaluating the scales' validity. In addition, it could improve and foster cross-study comparison and enhance understanding of contextual influences on privacy, security and trust measures.

5.2.3. Reported scale reliability and validity

To address the fourth research question and investigate reliability and validity scores that were reported on privacy, security and trust metrics in the context of CAI. Therefore, an evaluation framework developed by Rohan et al. (2023) was used to assess information security scales. Their framework draws from widely accepted research on scale development and evaluation and can be generally applied to assess the reliability and validity of measurement scales. This framework was only applied to studies relying on multi-item scales, as commonly used reliability measures such as Cronbach's alpha require at least two items. The total scores on scale validation, i.e., reliability and validity, are calculated as follows: Reliability testing is based on the calculation of Cronbach's alpha and composite reliability each contributing 0.5 to a possible full score of 1. Convergent validity assessment is again based on two measures, namely on factor loadings and average variance extracted (AVE) coefficient. Finally, a full score of 1 is given if discriminant validity has been assessed by the study. Thereby, the respective values need to be within widely accepted thresholds, e.g. above 0.7 for Cronbach's Alpha. It needs to be mentioned that for trust and privacy & security scales, none of the papers reported values outside their threshold. If papers initially found reliability or validity issues, measures were taken to resolve them.

Table 8
Reliability and validity assessment of papers using multi-item scales based on a framework by Rohan et al. (2023). Individual assessments of the scales are shown in the Appendix in Tables 16 and 17. The overall percentage was computed by averaging the individual scores per paper.

Fulfilled criteria	Internal consistency	Discriminant validity	Convergent validity
Privacy & security	76%	63%	63%
Trust	45%	27%	27%

We want to highlight that by applying this framework we do not judge the overall quality of reviewed studies. Instead, our analysis serves the purpose of evaluating and deepening our understanding of privacy, security and trust perception scales used in the context of CAI. While we acknowledge that reliability and validity measures can take various forms, the framework helps to assess whether researchers followed best practices of scale validation. This is crucial as research on privacy, security and trust can have serious consequences in informing businesses and policymaking.

Table 8 shows the total scores for the validation of internal consistency, discriminant validity and convergent validity for privacy & security and trust scales. The individual assessments of the scales can be found in the Appendix in Tables 16 and 17. The overall percentage was computed by averaging the individual scores per paper based on the framework provided by Rohan et al. (2023). As previously mentioned, we only considered papers that used multi-item scales. Therefore, 100% would have been achieved if all papers using multi-item scales had calculated internal consistency as required by the framework.

First, there is a drastic difference between papers extracted by our SLR on security and privacy perceptions and the one on trust. Research on privacy and security perceptions assessed reliability and validity almost twice as often as research on trust perceptions in the context of CAI. Moreover, two different trends are observable. First, for the literature on trust, it was found that 25% of the papers calculated only Cronbach's alpha resulting in overall values of 0.5 for the measure of internal consistency. In contrast, papers evaluating privacy and security perceptions predominantly evaluated both, Cronbach's alpha and composite reliability, resulting in values of 1 for internal consistency evaluation. Thus, in total, 60% of papers sufficiently assessed the scale's reliability.

Second, for both literature reviews, it was observable that validity was only evaluated in cases in which also internal consistency was assessed. In turn, reliability was assessed the most to validate privacy, security and trust scales. Interestingly, for research on privacy perceptions, the assessment of reliability and validity measures is highly correlated with structural equation modeling methods for data analysis. This makes sense as structural equation modeling requires explicit quality assessment of the measurement model (Hair et al., 2021). These findings show that reliability testing seems to be the default while validity testing is not. Therefore, studies on privacy, security and trust perceptions could benefit from the well-established practices in the context of structural equation modeling to ensure the usage of valid and reliable scales.

5.3. Privacy, security and trust as an influence on CAI adoption

Roughly one-third of reviewed papers on privacy and security perceptions assessed perceptions in the context of CAI adoption. They predominantly drew upon the Technology Acceptance Model (TAM) or related conceptual frameworks. This does not hold for trust research, which only includes TAM in about 15% of studies. Nonetheless, TAM studies considered the constructs of trust and privacy & security in combination and are thus, investigated more closely on their interplay between trust, privacy and security. An overview of the studies along with their assessed variables is provided in Tables 9 and 10. It is crucial to highlight that all of the studies are based on one or more existing research model and usually provide insightful extensions to these frameworks in the context of CAI. The underlying research models (as shown in Tables 9 and 10) have been extracted from the descriptions and references found in the respective papers. Thereby, we only consider studies that explicitly stated that they built upon or extended an existing model.

5.3.1. Technology Acceptance Model (TAM)

The Technology Acceptance Model is one of the major frameworks for understanding factors affecting the potential adoption of technology (Marangunić & Granić, 2015). At its core, the basic TAM explains the adoption of a system through three key factors: ease of use, perceived usefulness and attitude towards usage. We identified 13 studies that build upon the original TAM to investigate adoption factors of CAI systems including various privacy, security and trust constructs. While the majority treats these constructs as independent variables, Cha, Wi, Park, and Kim (2021) hypothesize that perceived privacy risks not only negatively influence the intention to adopt smart speakers but also exert a moderating effect. Their findings reveal cultural differences between South Korean and US samples. In a unique contribution, Acikgoz and Vega (2022) assesses the relatively novel concept of privacy cynicism and its impact on attitude and trust in the context of CAI systems. Surprisingly, their findings indicate that privacy cynicism negatively influences attitudes towards voice assistant usage but contrary to existing literature positively affects users' trust. In addition to purely quantitative TAM studies, Tennant, Allana, Mercer, and Burns (2022) conducted a mixed-method study on caregivers' expectations of voice assistants in home care and rely on TAM to analyze their qualitative findings.

Finally, a study by Dekkal et al. (2023) draws on TAM but concentrates mainly on factors typically overlooked in common technology acceptance models. They explore drivers such as practicity, personalization and enjoyment as well as inhibitors, such as privacy concerns and creepiness, influencing trust and adoption in insurance chatbots. They find that privacy concerns do not significantly influence trust while creepiness does. Furthermore, both privacy concerns and creepiness have a marginal influence on adoption intention. In resonance with previously discussed studies, trust lacks a significant effect on adoption intention but is influenced by a moderating impact of technological anxiety.

Table 10 provides an overview of studies that contrast or incorporate other conceptual models into the TAM framework. Rese, Ganster, and Baier (2020) contrast TAM and the Uses and Gratifications Theory (U&GT) in the context of chatbot adoption in online retailers and find that both models showed similar predictive power. Kwangsawad and Jattamart (2022) integrates TAM and Diffusion of Innovation theory (DOI) to evaluate consumers' intention to utilize chatbot services. Meanwhile, Patil and Kulkarni (2022) builds on TAM and the Health Belief Model (HBM) to examine the use of health and wellness chatbots considering factors such as severity of potential health problems and benefits and barriers to chatbot adoption. Another study combines TAM and the Information Systems Success Model (D&M) to validate the acceptance of cognitive chatbots in a B2B context. They confirm that privacy risks have a moderating effect on aspects of information system quality. Finally, Pitardi and Marriott (2021) draw from various theories including human–computer interaction theories and para-social relationship theories such as the Extended Privacy Calculus Model (EPCM) and Service Robot Acceptance model (sRAM).

5.3.2. Unified Theory of Acceptance and Use of Technology (UTAUT)

As shown in Table 11, six reviewed papers build on the Unified Theory of Acceptance and Use of Technology (UTAUT) and UTAUT2 to examine adoption factors in the context of CAI. Developed by Venkatesh and Davis (2000), UTAUT and its successor UTAUT2, evolved through review, comparison and integration of technology acceptance models. Thereby, the original UTAUT includes constructs on performance expectancy, effort expectancy, social influence and facilitating conditions to influence behavioral intention and thus, actual use of technology. In the context of virtual assistants for cancer patients, van Bussel, Odekerken-Schröder, Ou, Swart, and Jacobs (2022) deployed UTAUT by introducing additional factors such as self-efficacy, trust and resistance to change.

Four papers build on UTAUT2 in the context of CAI systems which modifies and extends UTAUT by introducing three new constructs: hedonic motivation, price value and habit (Venkatesh, Thong, & Xu, 2012). For instance, García de Blanes Sebastián, Sarmiento Guede, and Antonovica (2022) found that trust significantly impacts users' intention to use virtual assistants while perceived privacy risks did not show the same influence. Similarly, Vimalkumar et al. (2021) examined the adoption of voice-based digital assistants based on an extension of UTAUT2. Notably, they are among the few to explicitly examine the relationship between perceived trust, perceived privacy risks and perceived privacy concerns. Their results show that perceived privacy risks significantly influence perceived privacy concerns and trust. In line with García de Blanes Sebastián et al. (2022), they find that perceived trust does positively influence behavioral intention while perceived privacy risks do not. Moreover, they discovered that perceived privacy concerns do not significantly impact behavioral intention.

In a distinct approach, Pal, Roy, Arpnikanondt and Thapliyal (2022) integrate UTAUT2 with parasocial relationship theory (PSR) and privacy aspects to investigate behavioral intention to use voice-based consumer electronic devices. Their results suggest that perceived privacy risks significantly influence perceived privacy concerns and trust. Yet, in stark contrast to previous research, they found that trust did not significantly influence behavioral intention. Additionally, they observed that privacy concerns did not significantly influence trust.

Generally, these findings suggest that perceived privacy risk may not have a direct influence on adoption but may be mediated through consumer trust (Vimalkumar et al., 2021). Nevertheless, the studies also reveal conflicting results concerning the influence of trust on behavioral intention to use CAI systems. Their research specifically highlights the importance of a comprehensive assessment of privacy, security and trust constructs to enhance understanding of adoption factors within the context of CAI systems considering diverse situations and user groups.

5.3.3. Other conceptual models

Some of the reviewed papers investigate the adoption of CAI systems drawing insights from various other conceptual models as shown in Table 12. Han and Yang (2018) extend the Parasocial Relationship theory (PSR) to investigate factors influencing adoption intentions. They find that privacy and security risks negatively affected parasocial relationships. Shofolahan and Kang (2018) build upon the Value-based Adoption Model (VAM) taking into account factors such as perceived security risk, perceived technicality, perceived cost as well as perceived usefulness and enjoyment. Surprisingly, only perceived cost was found to negatively influence perceived value while security risk and technicality do not. Along similar lines, Cao et al. (2022) explores the adoption intention of voice assistants among Airbnb guests by drawing on the Self-Efficacy based Value Adoption Model (SVAM) and identified privacy risks as a significant determinant.

Table 9
Overview of studies in our reviewed sample that build upon and extend the Technology Acceptance Model (TAM) to research adoption intention in the context of privacy, security and trust perceptions. Only studies that explicitly stated the reliance or extension of TAM are considered. Detailed explanations are provided in Section 5.3.1.

Underlying research model	Independent variable(s)	Moderating variable	Mediating variable	Dependent variable	Reference
TAM	Technology optimism, System diversity, System quality, Perceived enjoyment, Perceived usefulness, Perceived ease of use, Risk, **Surveillance anxiety**, **Security/Privacy risk**			Behavioral intention	Kowalczuk (2018)
TAM	Perceived usefulness, Perceived ease of use, Attractiveness, **Trust**, **Mistrust**, Hedonic quality, Pragmatic quality, **Perceived security**			Intent	Fahn and Riener (2021)
TAM	Perceived usefulness, Perceived ease of use, Attitude, **Trust perception**			Usage intention	Choung et al. (2023)
TAM	Perceived usefulness, Perceived ease of use, Perceived enjoyment, Price consciousness, **Perceived Risk**, **Trust**, Personal innovativeness		Attitude	Intention to use	Kasilingam (2020)
TAM	Perceived usefulness, Perceived ease of use, Personal norms, Societal norms, **Privacy concerns**, **Perceived security**		Attitude toward using voice assistants	Intention to use	Buteau and Lee (2021)
TAM	Perceived usefulness, Perceived ease of use, **Perceived privacy risk**, Innovativeness, Perceived enjoyment, Social attraction, Task technology fit		Attitude towards smart speakers	Intention to use	Aiolfi (2023)
TAM	Perceived usefulness, Perceived ease of use, **Privacy cynicism**		**Trust towards using VAs**, Attitude towards VAs	Habit of using	Acikgoz and Vega (2022)
TAM	Perceived usefulness, Perceived ease of use, Perceived enjoyment, **Perceived privacy risks**	**Perceived privacy risks**		Adoption intention	Cha et al. (2021)
TAM	Perceived ease of use, **Perceived trust**, Perceived enjoyment, Perceived usefulness			Behavioral intention to use	Jameel and Karem (2022)
TAM	Perceived usefulness, Perceived ease of use, Perceived enjoyment, Information quality, Service quality, Interface and design, **Perceived risk**, Structural assurances, **Privacy and security concerns**, **Disposition to trust**, Technology fear, Ubiquity		**Chatbot trust**	Attitude, Intention, Customer satisfaction	Alagarsamy and Mehrolia (2023)
TAM	Perceived usefulness, Perceived ease of use, **Perceived privacy risk**, Perceived compatibility, Awareness of service			Behavioral intention to use	Alt and Ibolya (2021)
TAM	Perceived usefulness, Perceived ease of use, **Concerns**, Excitement, cost, Prior experience			Attitudes towards use	Tennant et al. (2022)
TAM	Practicity (Perceived ease of use/Perceived usefulness), Personalization, Enjoyment, **Privacy concerns**, Creepiness	Technology anxiety	**Trust**	**Trust**, Adoption intention	Dekkal et al. (2023)

5.4. Beyond adoption: Influence on privacy, security and trust on usage, disclosure and more

In addition to theoretical models that examine the influence of privacy, security and trust perception on the adoption of CAI systems, we identified various studies that did not build upon TAM, UTAUT or UTAUT2 and investigated variables beyond adoption such as usage or disclosure. Thereby, they do not always build upon theoretically grounded research models but conceptualize and validate individual models.

5.4.1. Usage, disclosure and attitude

Table 13 provides an overview of reviewed papers investigating usage, disclosure and attitude towards CAI systems. Uses and Gratification Theory (U&GT) is among the mostly employed theories to understand usage intention in our sample. For instance, McLean and Osei-Frimpong (2019) explore utilitarian, hedonic and symbolic benefits in addition to social benefits such as social presence and attraction and their impact on voice assistant usage. Their findings suggest positive effects on voice assistant use across all factors with perceived privacy risks exerting a significant negative moderating effect. Another study drawing on U&GT investigated continuance use intentions of virtual assistants across generations and identified a non-linear relationship between privacy concerns and generations (Kefi et al., 2021). Lee et al. (2020) explore the effect of habit and continuance use on the perception of group harmony in situations where voice assistants are shared. In addition, they examine hedonic motivation, compatibility and perceived security as antecedents to satisfaction. Their results indicate that perceived security influences satisfaction only marginally while habit and continuance use significantly impact group harmony in a multi-person context. Similarly, in the context of chatbots, Cheng and Jiang (2020) found that privacy risks negatively influence satisfaction. In turn, satisfaction positively affects both continued use and customer loyalty. Three studies do not rely on U&GT to investigate usage. Instead, Lee, Sheehan et al. (2021) extends the Post-Acceptance Model of Information System Continuance (PAMISC) to investigate the influence of personal traits on the continuation and recommendation intention of voice assistants. They found that perceived security had no significant influence on satisfaction possibly a result of investigating continuance intention rather than initial adoption intention. Based on their own conceptualization, Pal, Babakerkhell et al. (2022) show that both cognitive as well as emotional trust significantly influence the usage of voice assistants. Interestingly, as opposed to the hypothesis, perceived anthropomorphism did not significantly affect emotional trust.

Three studies explore the impact of privacy and trust on self-disclosure in the context of CAI. Lappeman et al. (2023) investigate three dimensions of trust and privacy concerns in financial chatbots

Table 10
Overview of studies in our reviewed sample that contrast or extend the Technology Acceptance Model (TAM) with other conceptual frameworks to research adoption intention in the context of privacy, security and trust perceptions. Only studies that explicitly stated the reliance or extension of the underlying research model are considered. Detailed explanations are provided in Section 5.3.1.

Underlying research model	Independent variable(s)	Moderating variable	Mediating variable	Dependent variable	Reference
TAM, UTAUT	Perceived usefulness, Perceived ease of use, Social influence, Hedonic motivation, **Perceived privacy concerns, Perceived trust**			Behavioral intention to use	Muñoz and Kremer (2023)
TAM, U&GT	Perceived usefulness, Perceived ease of use, Convenience, Authenticity of conversation, Enjoyment, Pass time, **Privacy concerns**, Immature technology			Behavioral Intention to use	Rese et al. (2020)
TAM, IDP	Perceived time risk, **Perceived privacy risk**, Perceived usefulness, Perceived ease of use, Perceived convenience, Perceived information quality, Technological anxiety, Openness to experience		Attitude toward continued	Intention	Kwangsawad and Jattamart (2022)
TAM, HBM	**Propensity to trust technology**, Social influence, Perceived usefulness, Perceived ease of use, **Privacy**, **Safety risk**, Facilitating condition, Perceived susceptibility, Perceived severity, Perceived benefit, Perceived barrier		**Trust belief in technology**	Adoption intention	Patil and Kulkarni (2022)
TAM, D&M	Perceived information quality, Perceived system quality, Perceived service quality, Perceived ease of use, Perceived usefulness, **Perceived trust**	**Perceived risk**	Customer experience, Attitude towards technology	Adoption intention	Behera, Bala, and Ray (2021)
TAM, SRAM, EPCM	Perceived usefulness, Perceived ease of use, Enjoyment, Social presence, Social cognition, **Privacy concern**		Attitude, **Trust**	Intention to use	Pitardi and Marriott (2021)
TAM, SRAM, EPCM	Behavioral traits, Humanlike traits		Perceived usefulness, Perceived ease of use, Social presence, **Trusting belief**	Continued usage intention	Prakash et al. (2023)
TAM, SRAM	Perceived usefulness, Perceived ease of use, Perceive humanity, Perceived social interactivity, Perceived social presence		**Trust**	Acceptance of artificial intelligence virtual assistant	Zhang, Meng, Chen, Yang, and Zhao (2021)

Table 11
Overview of studies in our reviewed sample that build on the Unified Theory of Acceptance and Use of Technology (UTAUT) and UTAUT2 framework to research adoption intention in the context of privacy, security and trust perceptions. Detailed explanations are provided in Section 5.3.2.

Underlying research model	Independent variable(s)	Moderating variable	Mediating variable	Dependent variable	Reference
UTAUT	Self-efficacy, Performance expectancy, Effort expectancy, Social influence, Facilitating conditions, **Trust**, Resistance to change		Effort expectancy	Behavioral intention	van Bussel et al. (2022)
UTAUT	Effort expectancy, Effort expectancy, **Perceived security**, Social influence, Facilitating condition, Perceived anthropomorphism, Perceived animacy, Perceived intelligence		Parasocial interactions, Smart-Shopping perception, AI-Enabled customer experience	Continuance intention	Aw et al. (2022)
UTAUT2	Performance expectancy, Effort expectancy, Social influence, Facilitating conditions, Hedonic motivation, Price value, Habit, **Privacy concerns**			Intention to use	Farooq, Jeske, van Schaik, and Moran (2022)
UTAUT2	Performance expectancy, Effort expectancy, Social influence, Facilitating conditions, Personal innovativeness, **Trust**, **Perceived privacy risk**, Hedonic motivation, Habit, Price/Value			Behavioral intention	García de Blanes Sebastián et al. (2022)
UTAUT2	Performance expectancy, Effort expectancy, Social influence, Hedonic motivation, Price/Value, Facilitating conditions, **Perceived privacy risks**		**Perceived trust**, **Perceived privacy concerns**, Behavioral intention	Adoption	Vimalkumar et al. (2021)
UTAUT2, PSR	Performance expectancy, Effort expectancy, Hedonic motivation, **Perceived privacy risk**, Perceived social presence, Perceived humanness, Social cognition		**Perceived privacy concern**, **Trust**	Behavioral intention	Pal, Roy et al. (2022)

suggesting that while privacy concerns negatively influence users' self-disclosure, brand trust was not found to influence self-disclosure in South Africa. In another study, Ischen et al. (2020) compared two types of chatbots, i.e. human-like, machine-like chatbots, and a traditional website concerning privacy concerns and information disclosure. Their findings show that the human-like chatbot led to higher perceived anthropomorphism and fewer privacy concerns, consequently resulting in higher information disclosure in comparison to machine-like chatbots. Yet, the results do not hold when compared to a common website. Finally, Cho (2019) investigate the effect of modality and device on users' perceived social presence and attitude towards voice assistants including usability aspects. They found that voice positively

Table 12
Overview of studies in our reviewed sample that build on conceptual models beyond TAM, UTAUT and UTAUT2 to research adoption intention in the context of privacy, security and trust perceptions. Detailed explanations are provided in Section 5.3.3.

Underlying research model	Independent variable(s)	Moderating variable	Mediating variable	Dependent variable	Reference
PSR	Task attraction, Social attraction, Physical attraction, **Security/Privacy risk**		Parasocial relationship, Satisfaction	Adoption intention	Han and Yang (2018)
VAM	Perceived usefulness, Perceived enjoyment, **Perceived security risk**, Perceived Technicality, Perceived cost, Social influence, Usage	Gender	Perceived value	Adoption intention	Shofolahan and Kang (2018)
SVAM	Self-efficacy, Functional value, Emotional value, Social value, **Privacy risk**			Adoption intention	Cao, Sun, Goh, Wang, and Kuiavska (2022)

Table 13
Overview of studies in our reviewed sample that research privacy, security and trust perceptions in the context of usage, disclosure and attitude towards conversational AI systems. Detailed explanations are provided in Section 5.4.1.

Underlying research model	Independent variable(s)	Moderating variable	Mediating variable	Dependent variable	Reference
U&GT	Utilitarian benefits, Hedonic benefits, Symbolic benefits, Social presence, Social attraction	**Perceived privacy risk**		Usage	McLean and Osei-Frimpong (2019)
U&GT	Utilitarian uses, Hedonic uses, Subjective norms, Perceived critical mass, **Perceived privacy concerns**	**Perceived privacy concerns**		Continuance use intention	Kefi, Besson, Sokolova, and Aouina-Mejri (2021)
U&GT	Information, Entertainment, Media appeal, Social presence, **Privacy risk**		Satisfaction, Customer loyality	Continued use intention	Cheng and Jiang (2020)
U&GT, Signaling and prospect theory	Utility features, Hedonic features, Social presence, **Perceived privacy risk**	Gender, Brand credibility	Overall perceived value	Continued usage intention	Jain, Basu, Dwivedi, and Kaur (2022)
U&GT, Signaling and prospect theory	Utility features, Hedonic features, Social presence, **Perceived privacy risk**, Irritation	Gender, Brand credibility, Irritation	Perceived value	Continued usage intention, Brand's loyalty	Maroufkhani, Asadi, Ghobakhloo, Jannesari, and Ismail (2022)
PAMISC	Personal innovativeness, Technology anxiety		Confirmation, privacy value, Hedonic motivation, Compatibility, Perceived security, Satisfaction	Continuance intention, Intention to recommend others	Lee, Sheehan, Lee and Chang (2021)
n.a.	Hedonic motivation, Compatibility, **Perceived security**, Diversity use		Satisfaction, habit	Continuance use	Lee, Lee, and Sheehan (2020)
n.a.	**VAPA privacy concern**, **Household members privacy concern**, **Government privacy concern**, **Vendor and third party privacy concern**, Perceived anthropomorphism, Perceived intelligence	Perceived intrusiveness	**Emotional trust**, **Cognitive trust**	Usage of VAPA's	Pal, Babakerkhell et al. (2022)
SCM, RFT	Regulatory focus, Interaction style		**Trust**	Willingness to self-disclose	Choi and Zhou (2023)
Saffarizadeh, Boodraj, Alashoor, et al. (2017)	**Brand trust**, **Digital privacy concerns**		**Cognitive trust**, **Emotional trust**	User self-disclosure	Lappeman et al. (2023)
n.a.	Human-like chatbot vs. Machine-like chatbot vs. Website,		**Privacy concerns**, Perceived anthropomorphism	Information disclosure, Attitudes, Recommendation adherence	Ischen, Araujo, Voorveld, Van Noort, and Smit (2020)
n.a.	Modality	**Privacy concerns**	Perceived social presence	Attitude toward the voice assistant	Cho (2019)

contributes to social presence and thus, a positive attitude towards the assistant only under certain circumstances, i.e., low information sensitivity and low privacy concerns, suggesting that text-based interactions can similarly induce human-like perceptions.

Generally, these findings imply a transferability of insights from conceptual models developed for text-enabled CAI systems to investigating adoption, usage and other patterns in voice-based CAI systems. Factors like privacy risks seem to continuously impact satisfaction and thus usage of assistants while the interplay of anthropomorphic factors, modality and perceptions requires further investigation. As voice-based CAI systems continue to evolve, drawing from previous work on text-based CAI and traditional interactive systems can guide researchers and contribute to a more comprehensive understanding of factors shaping perceptions in the CAI context.

5.4.2. *Advertising, brand loyalty and privacy management*

Table 14 provides an overview of studies employing conceptual models to research privacy, security and trust perceptions in the context of privacy management, advertising, and brand loyalty. Only one paper investigated potential advertising acceptance in smart speakers. Guerreiro, Loureiro, and Ribeiro (2022) show that usefulness and hedonic motivations significantly influence advertising acceptance with a moderating effect of privacy risks on smart speaker usefulness. In a case study on Siri and an investigation on brand loyalty, Hasan, Shams,

Table 14
Overview of studies in our reviewed sample that research privacy, security and trust perceptions in the context of privacy management, advertising and brand loyalty in conversational AI systems. Detailed explanations are provided in Section 5.4.2.

Underlying research model	Independent variable(s)	Moderating variable	Mediating variable	Dependent variable	Reference
SOR	Perceived warmth, Communication delay, Perceived competence, communal relationship, Exchange relationship		**Trust in chatbots**	Intention to switch	Cheng, Zhang, Cohen, and Mou (2022)
U&GT, Media equation, CPM	Personal utility, Info seeking, Relaxation, Enjoyment, Status, Music exploration, Multitasking		**Privacy concerns**, Medium-as-social-actor presence	**Privacy setting review**, **Ownership protection**	Xu et al. (2022)
SOR	Privacy concerns		Emotional reactions	Problem-focused coping, Emotion-focused Coping	Park et al. (2021)
n.a.	**Perceived trust**		Controllability, Perceived performance, Bidirectionality, synchronicity	Customer satisfaction	Purwanto et al. (2020)
n.a.	smart Speaker Ease of use, Advertising functionality, Advertising relevance, Advertising format	**Privacy risk**	Smart speaker usefulness, Hedonic motivation	Advertising acceptance	Guerreiro et al. (2022)
n.a.	**Trust**, Interaction, **Perceived risk**, Novelty value			Brand loyalty	Hasan et al. (2021)

and Rahman (2021) show that perceived risks negatively affect brand loyalty. Interestingly, this effect is moderated by employment with a greater negative influence observed for unemployed consumers. Furthermore, Xu, Chan-Olmsted, and Liu (2022) investigated the effect of gratification on privacy concerns and medium-as-social actor presence and their effects on privacy setting review and ownership protection. Their findings suggest that personal utility, relaxation, enjoyment and status affected privacy concerns. Moreover, privacy concerns had a positive effect on both privacy setting review and ownership protection.

As CAI systems continue to be integrated further into everyday life, researchers need to move beyond factors influencing adoption and usage. Therefore, gaining insights into factors shaping advertising acceptance and the acceptance of privacy management options in the context of CAI systems is crucial to advancing technologies and formulating design recommendations. While our review uncovered only a limited number of studies investigating these factors based on conceptual and theoretical models, future work should deepen understanding in these domains.

5.4.3. Trust as a dependent variable

Next to gathering trust as a direct item in questionnaires, seven papers used trust as the dependent variable (as shown in Table 15). Due to the difficulty of defining trust, the objective of these studies was either to find antecedents to trust and their influence on trust or to use proxies instead of trust. For instance, in Gulati, Sousa, and Lamas (2018), the antecedents of trust and their impact on user trust were investigated. Müller et al. (2019) took a different approach and focused on which character profiles show the highest trust towards chatbots. This was based on the HEXACO personality profile (Lee & Ashton, 2004) which is an extension to the well-known Big Five personality traits. This stands in line with the studies using trust as a mediating variable, where the independent variable was mostly antecedents of trust with an additional dependent variable.

It seems beneficial to use proxies, or additional measures of trust in the collection of trust as they provide a context into the study as well as being more straightforward to grasp. For example, predictability, or reputation are concepts which seem more natural to reflect on.

5.5. Tools for privacy, security and trust perception manipulation

In this section, we specifically highlight the tools used to manipulate privacy, security and trust perceptions. While a majority of studies focused on quantitative methods applying surveys, a significant sample conducted experiments in quantitative or mixed-method settings to understand users' perceptions.

A majority of these studies relied on commercially available voice-based CAI systems such as Amazon Echo, Google Assistant or Siri (Cho, 2019; Cowan et al., 2017; Rajapaksha et al., 2021). Other studies investigated users' perceptions on text-based CAI systems using broker-bots or Facebook e-commerce chatbot (Kasilingam, 2020; Lee, Frank & IJsselsteijn, 2021)

Few studies did not rely on existing chatbots or voice assistants but implemented their own CAI applications using Microsoft's Power Virtual Agent Platform, IBM Watson Platform, specifically developed Amazon Alexa applications, Chatbot Language (CBL), or a conversational agent research toolkit developed by Araujo (Brüggemeier & Lalone, 2022; Casadei, Schlögl, & Bergmann, 2022; Cho et al., 2020; Dekkal et al., 2023; Fahn & Riener, 2021; Gauder et al., 2023; Ischen et al., 2020).

More advanced CAI prototypes were developed by studies investigating individual digital study assistants (König, Karrenbauer, & Breitner, 2023) as well as authentication methods and privacy controls (Mhaidli, Venkatesh, Zou, & Schaub, 2020; Renz et al., 2023). For instance, Renz et al. (2023) implemented a fake voice-banking application for Google Home Mini and four different authentication methods. Mhaidli et al. (2020) developed a smart speaker prototype implementing two privacy controls based on gaze direction and voice volume level and investigated users' perceptions in a lab study.

Additionally, we found vignette studies to be implemented frequently in trust research (Gupta et al., 2019; Li, Kamaraj & Lee, 2023; Toader et al., 2019; Wald, Heijselaar, & Bosse, 2021). This was prevalent, especially in studies that implemented their own chatbot or voice assistant and common among studies that conducted in-lab experiments. We could also observe that those studies, which use a vignette study did not directly implement a trust scale but focused on either trust measurement from other sources (for instance audio directly) (Li, Erickson, Cross and Lee, 2023), or studies which investigated the effect of style and intonation on trust (Tastemirova et al., 2022).

Other methods to investigate privacy, security and trust perceptions included the usage of experience sampling methodology. Here, Malkin et al. (2019) implemented a browser extension to play back historical voice recordings to voice assistant users. Moreover, we need to highlight the rare utilization of long-term studies in the context of CAI.

Table 15
Overview of studies in our reviewed sample that use trust or trustworthiness as the dependent variable. Detailed explanations are provided in Section 5.4.3.

Underlying research model	Independent variable(s)	Moderating variable	Mediating variable	Dependent variable	Reference
SPT	Motivation, Competence, Benevolence, Predictability, Honesty, Reciprocity, Structural assurance, Willingness			**Trust**	Gulati et al. (2018)
n.a.	Emotional experiences		Social presence	**Trust**	Lee and Sun (2022)
n.a.	Expertise, Predictability, Human-likeness, Ease of use, **Risk**, Reputation, **Propensity to trust technology**			**Trust**	Nordheim et al. (2019)
n.a.	Human-like cues, Tailored responses, Task creativity, Ambiguity		Social presence, Perceived task solving competence	**Trust toward chatbot**	Jiang et al. (2023)
n.a.	Emotion, Emotion intensity			Perceived affect, Perceive sincerity, **Perceived trustworthiness**, Overall perception	Tastemirova, Schneider, Kruse, Heinzle, and Brocke (2022)
HEXACO	Honesty, Emotionality, Extraversion, Agreeableness, Conscientiousness, Openness anthropomorphic design cues		Social presence, Perceived competence	Positive consumer response, **Trust**	Müller et al. (2019)
n.a.	System quality		Subjective norm, Familiarity, Technology optimism, Perceived enjoyment	**Perceived trust**	Liu, Gan, Song, and Liu (2021)

Noteworthy, Choi, Thompson, and Demiris (2020) conducted a two-month feasibility study with older adults using IoT smart home devices including smart speakers.

It is to be noted that a few studies did not engage in any interaction with a voice assistant but rather were based on prior experiences with a common assistant or a short video about an interaction was shown before the survey (Cha et al., 2021; Müller et al., 2019; Purwanto et al., 2020; Weidmüller, 2022). Others relied on measurement aids depicting simulated chatbot conversations to manipulate experimental conditions (Lappeman et al., 2023). Further, scenario-based designs were utilized for example to present virtual prototypes of voice assistants and to investigate users' perceptions concerning privacy controls (Ahmad et al., 2022).

6. Discussion

We conducted a systematic literature review on empirical methods and privacy, security and trust perception measures in the context of CAI. While the interplay of privacy, security and trust perceptions has been long discussed in the context of new technology, we uniquely contribute to the literature by providing a joint perspective on privacy, security and trust perception measurements and by focusing on CAI systems including both voice- and text-based systems.

First, our review sheds light on methods used to research users' perceptions in the context of CAI (**RQ1**). We found that quantitative research methods in particular dominate the field of trust perceptions while privacy and security perceptions are – in addition to quantitative methods – frequently explored through qualitative and mixed-methods studies. Given that privacy and trust perceptions are highly contextual, qualitative and mixed-method studies might be particularly helpful in exploring why people respond a certain way (Barkhuus, 2012). Moreover, we extensively discussed the tools applied by researchers to expose participants to conversational assistants. While we found a significant sample of reviewed papers to implement applications or develop prototypes, the majority relied on peoples' previous experiences with CAI systems or scenario-based experiments to evaluate privacy, security and trust perceptions. Moreover, we found strong reliance on commercially available systems when implementing prototypes which could impose research constraints and hinder research on innovative solutions. This is especially true since the brand or company behind commercially available systems might have a significant influence on privacy and trust perceptions. Thus, our findings suggest that the field could generally profit from the diversification of research methods and research-friendly methods to implement CAI systems.

Second, we were interested in which constructs are assessed and which scales are used when users' perceptions of privacy, security and trust are investigated in the context of CAI systems (**RQ2 and RQ3**). Our review shows that the most prevalent constructs in this domain are trust, privacy concerns, anthropomorphic aspects and risk perceptions. Nevertheless, our extensive analysis shows that various sub-constructs are commonly assessed such as various types of privacy concerns or trust. While a more fine-grained assessment can enhance our understanding of people's perceptions, a clear distinction between these concepts might not be reflected in the associated scales possibly leading to conflicting research outcomes (Colnago et al., 2022). At the same time, constructs are referred to interchangeably increasing the risk of unreliable outcomes. Privacy, security and trust research could benefit from grounding their assessment into already-existing theoretical frameworks and standards on definitions of privacy, security and trust.

Next, we were interested in the reported reliability and validity scores for privacy, security and trust metrics (**RQ4**). Therefore, we deployed a previously developed framework for scale validation and found significant differences between the fields of privacy & security and trust. Our findings reveal that reliability is most frequently assessed when compared to validity, particularly when conceptual models are evaluated using structural equation modeling. Therefore, we urge the research community to follow best practices of scale validation whenever scales are developed, reused or adapted.

Furthermore, our literature review focused on a joint investigation of privacy, security and trust perception measures (**RQ5**). Given previous research on the interplay of privacy, security and trust perceptions in online environments, we were interested to which extent these constructs have been jointly researched in the context of CAI. Surprisingly, we found only two papers that were identified by both our literature searches. Despite this finding, we discovered multiple papers jointly investigating privacy, security and trust perceptions, particularly often in the context of CAI adoption. This shows that current research on CAI adoption implicitly assumes a joint influence of these perceptions, yet, lacks explicit evaluation. Moreover, our research shows that a better understanding of the relationship between privacy, security and trust perceptions is required beyond adoption to inform the design of trustworthy and privacy-preserving CAI systems.

Finally, we were interested in which topics were investigated whenever privacy, security and trust perceptions were researched (**RQ6**). We found that a majority of papers investigated users' perceptions in relation to CAI adoption. Thereby, researchers relied on a multitude of conceptual frameworks and theories such as TAM or UTAUT. Despite the varying extensions explored in the reviewed studies, the prevalent use of TAM as an underlying research model is concerning. TAM does not explicitly model factors related to privacy, security and trust and the increased addition of factors makes comparability challenging. Conceptual models that integrate traditional technology acceptance frameworks with privacy and trust factors, such as the privacy-calculus acceptance models (Schomakers, Lidynia, & Ziefle, 2022), are essential for advancing research in the field and for the development of more complex and comprehensive frameworks while maintaining comparability. While investigated privacy and trust constructs were mostly limited to privacy risks and trust in general, they were treated non-uniformly as independent, moderating, mediating or dependent factors. Therefore, it is not surprising that results were found conflicting. Nevertheless, privacy and security risks were commonly treated as inhibitors while trust was expected to drive adoption. Future research could benefit from streamlining investigations and exploring factors beyond privacy risks and trust to better understand their impact on CAI adoption. Moreover, it will be crucial to further investigate factors beyond adoption.

7. Future research directions

We now want to highlight additional future research directions that have not yet been demonstrated and discussed in the previous section.

7.1. Diversification of application fields and user groups

Through our literature review, we identified application fields and user groups that have been investigated by the research community. We show that the majority of papers investigate CAI systems without a specific application focus. However, as privacy and trust perceptions are highly contextual, the application field can severely impact users' perceptions. Thus, research conducted in a general setting, might not be easily transferable to highly sensitive application fields such as finance. Future research should therefore diversify investigations across application fields to better understand users' privacy, security and trust perceptions in context. Furthermore, future work could investigate application fields that have not yet been covered such as exploring users' perceptions of CAI systems in the public sector or public places. Moreover, we found that comparisons of users' perceptions across multiple application fields is a largely unexplored area.

Next, our literature review sheds light on investigated user groups and participants. Generally, a strong reliance on crowdworking platforms was observable which can come with reliability and generalizability issues. The research community should critically discuss this trend and rely on traditional research and recruitment methods besides crowdsourcing. On the other hand, research on privacy and security perceptions has frequently focused on technology users while research on trust perception did not. In general, research on trust perceptions could benefit from the diversification of user groups, while the privacy and security field should intensify its efforts in recruiting different types of users.

7.2. Need for long-term evaluation

In our literature research on privacy and security, we discovered only one paper that investigated users' perceptions throughout two months (Choi et al., 2020). Long-term studies may be more complex and time-consuming, yet, can provide valuable insights compared to studies capturing snapshots of users' perceptions. Particularly, as privacy and trust perceptions are known to change over a period of time, long-term studies are vital for enhancing research in this domain. Thereby, researchers in the CAI domain could benefit from other research fields that frequently conduct long-term evaluations such as human–robot-interaction (De Graaf, Ben Allouch, & van Dijk, 2016; Fernaeus, Håkansson, Jacobsson, & Ljungblad, 2010).

7.3. Towards a unified privacy, security and trust scale

Previous work shows that well-established scales exist to measure privacy, security and trust perceptions (Jian et al., 2000; Lankton et al., 2015; Mayer et al., 1995; Preibusch, 2013). Yet, our literature research revealed that they are only rarely used to assess users' perceptions in the context of CAI. Therefore, it remains an open question whether they are sufficiently reliable and valid in the context of CAI or whether CAI-specific metrics are needed to evaluate privacy, security and trust perceptions. For example, the usability field has seen the emergence of CAI-specific usability scales to adapt to the unique capabilities of CAI (Zwakman et al., 2021). Future research could compare and validate multiple privacy, security and trust perception scales in the context of CAI and assess their suitability.

On a more general note, given the diversity of constructs in privacy, security and trust research, it might be worthwhile to explore adaptable and modular questionnaires to assess perceptions. Similar approaches exist to measure various aspects of usability of traditional interfaces and voice user interfaces (Schrepp & Thomaschewski, 2019). While they include aspects of trust, trustworthiness of content and risk handling, privacy and security constructs are not yet covered. A modular questionnaire is especially useful if surveys need to be adapted to particular research questions. As discovered in this literature review, adaptation of scales and various combinations of privacy, security and trust constructs are common when evaluating users' perceptions in the context of CAI. Therefore, future research could assess the suitability of a modular questionnaire for researching privacy, security and trust perceptions, identify relevant constructs and provide additional contextual information to ensure appropriate usage.

7.4. Distinction between privacy and security perceptions

Our literature research revealed that security perceptions are among the less often researched constructs, predominately in the context of security attacks or authentication methods. Moreover, our reviewed papers draw an inconclusive picture of whether people can sufficiently distinguish between privacy and security. Given people's confusion around security and privacy, we argue that a product's security should first and foremost be assessed objectively, e.g. by metrics and certification. We encourage the currently visible trend in that measurements of security perceptions may only be relevant to be assessed for a few applications e.g. when users are actively asked to test secure protection mechanisms or authentication tools. In contrast, we see the need for a clear distinction between security and privacy risks and peoples' perceptions thereof.

7.5. Impact of modality

In our literature review, we explicitly focused on text-based as well as voice-based conversational AI systems to cover the full range of disembodied systems interacting with humans in natural language. Nevertheless, we found that a majority of papers investigated voice-based CAI systems, particularly in the context of privacy and security perceptions. While it is obvious that voice-based systems come with increased privacy risks due to their constant listening capabilities, text-based systems can raise similar concerns regarding data handling and are worthwhile exploring. In addition, we discovered only a few papers that researched the impact of modality on users' privacy, security and trust perceptions. As differences in modalities did not always result in differences in user perceptions, further research is necessary to enhance understanding of the possible transferability of outcomes from one modality to another. Moreover, research on trust perceptions has investigated CAI systems in virtual reality - a modality that was found unexplored in the field of privacy and security.

7.6. Impact of privacy controls and authentication methods

Our literature review revealed only a few papers that evaluated privacy controls or authentication methods and their influence on users' perceptions. While we acknowledge that papers researching privacy controls for CAI systems, might not investigate privacy, security or trust perceptions and might therefore not be covered in our literature search, the limited number of papers in this domain is still surprising. In particular, none of the papers on privacy controls or authentication methods investigated users' trust. Therefore, it remains unclear to which extent privacy controls and privacy-enhancing features can positively influence users' trust in the context of CAI systems. Given peoples' increasing exposure to CAI systems, we urge the need for research on privacy controls in this domain and their impact on users' behavior and perceptions.

7.7. Impact of LLMs

The vast increase in the use of Large Language Models (LLM) and generative AI for CAI systems is foreseeable to influence users' perceptions. So far, our literature review has revealed only little research on privacy, security and trust perceptions in CAI systems leveraging LLM capabilities. Only one study was found that investigated the usage and perceptions of ChatGPT in an educational context (Tlili et al., 2023). However, it has to be noted that we conducted our literature research in the first half-year of 2023 and considered only peer-reviewed articles. Given the fast-changing and evolving field, it is likely that a literature search conducted at a later point had resulted in a different outcome. On the other hand, the rise of LLMs might make research on the influence of privacy and trust more difficult as these systems are blackbox models with limited transparency, controllability and reproducibility. Thus, studies in which only one variable is controlled might produce different outcomes due to the use of generative models. This makes the assessment of voice assistants or chatbots which use LLMs more difficult. For researchers, the training and fine-tuning of these models also become more expensive as larger amounts of processing power need to be available for fine-tuning and additional training (Kaddour et al., 2023).

8. Limitations

While our paper provides valuable insights into the use and development of privacy, security and trust scales in the context of CAI, we acknowledge several limitations of our work. First, from the multitude of names for voice assistants and no common naming convention, it is obvious that the literature review might be incomplete as other terms for CAI might not have been included in our keyword search. While we aimed to cover the most prominent terms through multiple iterations, generative models could potentially help in refining the keyword search to include less often used search terms. Secondly, we limited this work to disembodied conversational AI systems, thereby neglecting embodied systems, in particular robots. This can be a drawback since there has been extensive research on the social interaction between robots and humans. Future work could extend this review to include human–robot interaction and compare findings between embodied and disembodied agents. While we provided a summary of qualitative studies found by our literature search, our work has a strong focus on privacy, security and trust perception scales mostly used in quantitative research and mixed-methods studies. Similarly, behavioral measures or bio-signals were not covered in this work, as this work focused on the evaluation of users' perceptions. Nevertheless, measures of biological signals have been identified throughout this literature review such as Gupta et al. (2020), opening possibilities for future endeavors.

9. Conclusion

In this paper, we have conducted a systematic literature review on users' privacy & security perceptions and trust perceptions in the context of conversational AI. We specifically included both, voice-based as well as text-based systems. Our analysis includes an investigation of meta-information such as author's affiliation, participants, and researched devices as well as a breakdown of researched constructs. Moreover, we provide an overview of topics researched alongside privacy, security and trust perceptions. We found that a majority of studies focus on TAM models when researching privacy and trust perceptions. These are also the studies that include both concepts, privacy & security and trust at the same time. Further, we identified future research directions specifically urging the community to explicitly investigate the relationship between trust and privacy perceptions.

CRediT authorship contribution statement

Anna Leschanowsky: Writing – original draft, Visualization, Project administration, Methodology, Investigation, Formal analysis, Conceptualization. **Silas Rech:** Writing – original draft,Visualization, Project administration, Methodology, Investigation, Formal analysis, Conceptualization. **Birgit Popp:** Writing – review & editing. **Tom Bäckström:** Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgment

A part of this work was supported by "Designing Inclusive & Trustworthy Digital Public Services for Migrants in Finland (Trust-M)" (Grant Number: 353529) funded by the Strategic Research Council of Finland.

Appendix

See Tables 16–18

Table 16
Overview of privacy and security-related constructs used in mixed and quantitative studies. We display whether studies reused scales by showing the corresponding reference. We compute reliability and validity scores based on Rohan et al. (2023) as described in Section 5.2.3. "n.a" is used whenever studies did not rely on multi-item scales and thus, reliability and validity assessment was not possible.

Construct	Frequency	Reference paper	Reference construct	Reliability testing	Convergent validity	Discriminant validity
Privacy	3	Privacy (Furini et al., 2020)	Not reported	n.a.	n.a.	n.a.
		Privacy (Krey & Ramirez Garcia, 2022)	Not reported	n.a.	n.a.	n.a.
		Privacy (Patil & Kulkarni, 2022)	Faqih and Jaradat (2015)	1.0	1.0	1.0
Privacy perception	1	Privacy perception (Brüggemeier & Lalone, 2022)	Casaló, Flavián, and Guinalíu (2007)	0.0	0.0	0.0
Privacy concerns	40	General privacy concerns (Mols et al., 2022)	Vitak (2015)	0.5	0.0	0.0
		Mobile privacy concerns (Mols et al., 2022)	Xu, Gupta, Rosson, and Carroll (2012)	0.5	0.0	0.0
		Privacy concerns (Uysal et al., 2022)	Smith et al. (1996)	1.0	1.0	1.0
		General privacy concerns (Liao et al., 2019)	Vitak (2016)	0.5	0.0	0.0
		Privacy concerns (Cho et al., 2020)	Dinev et al. (2006)	0.5	0.0	0.0
		Privacy concerns (Alghamdi et al., 2022)	Not reported	0.5	0.0	0.0
		Privacy concerns (Joy et al., 2022)	Not reported	n.a.	n.a.	n.a.
		Device privacy concerns (Lutz & Newlands, 2021)	Not reported	0.5	0.0	0.0
		Household member privacy concerns (Lutz & Newlands, 2021)	Not reported	0.5	0.0	0.0
		Stranger privacy concerns (Lutz & Newlands, 2021)	Not reported	0.5	0.0	0.0
		Company privacy concerns (Lutz & Newlands, 2021)	Not reported	0.5	0.0	0.0
		Contractor privacy concerns (Lutz & Newlands, 2021)	Not reported	0.5	0.0	0.0
		Third-party privacy concerns (Lutz & Newlands, 2021)	Not reported	0.5	0.0	0.0
		Government privacy concerns (Lutz & Newlands, 2021)	Not reported	0.5	0.0	0.0
		Privacy concerns (Ng et al., 2020)	Ischen et al. (2020)	0.5	0.0	0.0
		Privacy concerns for multiple users (Lin & Parkin, 2020)	Not reported	n.a.	n.a.	n.a.
		Privacy concerns (Dekkal et al., 2023)	Malhotra, Kim, and Agarwal (2004)	0.5	1.0	1.0
		Privacy concerns (Buteau & Lee, 2021)	Dinev and Hart (2005)	1.0	0.5	1.0
		Perceived privacy concerns (Vimalkumar et al., 2021)	Alalwan (2020), Bansal, Zahedi, and Gefen (2016) and Smith et al. (2011, 1996)	1.0	1.0	1.0
		Privacy concern (Pitardi & Marriott, 2021)	McLean and Osei-Frimpong (2019)	1.0	1.0	1.0
		Perceived privacy concerns (Pal, Roy et al., 2022)	Alalwan (2020) and Smith et al. (2011)	1.0	1.0	1.0
		Privacy concerns (Abdi, Zhan, Ramokapane, & Such, 2021)	Malhotra et al. (2004)	0.0	0.0	0.0
		Privacy concerns (Cho, 2019)	Dinev et al. (2006)	0.5	0.0	0.0
		VAPA privacy concern (Pal, Babakerkhell et al., 2022)	Kowalczuk (2018)	1.0	1.0	1.0
		Household member privacy concern (Pal, Babakerkhell et al., 2022)	Kowalczuk (2018)	1.0	1.0	1.0
		Vendor & third-party privacy concern (Pal, Babakerkhell et al., 2022)	Kowalczuk (2018)	1.0	1.0	1.0
		Government privacy concern (Pal, Babakerkhell et al., 2022)	Kowalczuk (2018)	1.0	1.0	1.0
		Privacy concerns (Ischen et al., 2020)	Xu, Dinev, Smith, and Hart (2008)	0.5	0.0	0.0
		Privacy concerns (Xu et al., 2022)	Metzger (2007) and Quinn (2016)	0.5	0.0	0.0
		Privacy concerns (Lappeman et al., 2023)	Malhotra et al. (2004)	1.0	1.0	1.0
		Privacy concerns (Lv et al., 2022)	McLean and Osei-Frimpong (2019)	1.0	1.0	1.0
		Privacy concerns (Manikonda, Deotale, & Kambhampati, 2018)	Not reported	n.a.	n.a.	n.a.
		Privacy concerns (Malkin et al., 2019)	Not reported	n.a.	n.a.	n.a.
		Privacy concerns (Abrokwa, Das, Akgul, & Mazurek, 0000)	Gross (2021)	0.5	0.0	0.0
		Privacy concerns (Seymour, 2023)	Malhotra et al. (2004)	0.0	0.0	0.0
		Privacy concerns (Farooq et al., 2022)	Kim, Chung, and Lee (2011)	0.5	0.0	0.0
		Privacy concerns (Rese et al., 2020)	Rauschnabel, Rossmann, and tom Dieck (2017)	1.0	1.0	1.0
		Privacy concerns (Park et al., 2021)	Smith et al. (1996)	1.0	1.0	1.0
		Perceived privacy concerns (Muñoz & Kremer, 2023)	Pavlou (2003)	0.5	0.0	0.0
		Perceived privacy concerns (Kefi et al., 2021)	Xu et al. (2008)	0.5	1.0	1.0
Other concerns	7	Household IPA surveillance concerns (Mols et al., 2022)	Not reported	0.5	0.0	0.0
		Household IPA security concerns (Mols et al., 2022)	Not reported	0.5	0.0	0.0
		Household IPA platform concerns (Mols et al., 2022)	Not reported	0.5	0.0	0.0
		IPA data concerns (Liao et al., 2019)	Not reported	0.5	0.0	0.0
		Mobile data concerns (Liao et al., 2019)	Xu et al. (2012)	0.5	0.0	0.0
		Privacy and security concerns (Alagarsamy & Mehrolia, 2023)	Son and Kim (2008)	1.0	1.0	1.0
		Security and privacy concerns (Shlega, Maqsood, & Chiasson, 2022)	Van Deursen, Helsper, and Eynon (2016)	0.5	0.0	0.0
Control	8	Perceptions of control (Lin & Parkin, 2020)	Not reported	n.a.	n.a.	n.a.
		Previous privacy control usage (Lin & Parkin, 2020)	Not reported	n.a.	n.a.	n.a.
		Smart assistant privacy control usage (Lin & Parkin, 2020)	Not reported	n.a.	n.a.	n.a.
		Privacy control (Alghamdi et al., 2022)	Not reported	0.5	0.0	0.0
		Controllability (Purwanto et al., 2020)	Brill, Munoz, and Miller (2022)	1.0	1.0	1.0
		Perceived control (Pal et al., 2020)	Keith, Thompson, Hale, Lowry, and Greer (2013) and Mamonov and Benbunan-Fich (2018)	1.0	1.0	0.0
		Perceived control (Ahmad et al., 2022)	Hinds (1998)	0.0	0.0	0.0
		Privacy boundary control (Kang & Oh, 2023)	Child, Pearson, and Petronio (2009)	0.5	0.0	0.0

(*continued on next page*)

Table 16 (*continued*).

Construct	Frequency	Reference paper	Reference construct	Reliability testing	Convergent validity	Discriminant validity
Disclosure	6	Willingness to self-disclose (Kunkel, Donkers, Michael, Barbu, & Ziegler, 2019)	Ha, Chen, Uy, and Capistrano (2021)	0	0	0
		Willingness to self-disclose (Choi & Zhou, 2023)	Ha et al. (2021)	0.5	0	0
		Willingness (Gulati et al., 2018)	Pavlou and Gefen (2004)	1.0	1.0	1.0
		Personal information disclosure (Pal et al., 2020)		1.0	1.0	0.0
		User self-disclosure (Lappeman et al., 2023)		1.0	1.0	1.0
		Privacy disclosure (Kang & Oh, 2023)	Child et al. (2009)	0.5	0.0	0.0
Security	2	General security (McCarthy et al., 2020)	Not reported	n.a.	n.a.	n.a.
		Device security (Krey & Ramirez Garcia, 2022)	Not reported	n.a.	n.a.	n.a.
Security perception	9	Perceived security (Renz et al., 2023)	Not reported	n.a.	n.a.	n.a.
		Perceived security (Cho et al., 2020)	Salisbury, Pearson, Pearson, and Miller (2001)	0.5	0.0	0.0
		Security perception (Rajapaksha et al., 2021)	Not reported	n.a.	n.a.	n.a.
		Security perception (Brüggemeier & Lalone, 2022)	Casaló et al. (2007)	0.0	0.0	0.0
		Perceived security (Buteau & Lee, 2021)	Flavián and Guinalíu (2006)	1.0	0.5	1.0
		Perceived security (Fahn & Riener, 2021)	Cheng, Lam, and Yeung (2006)	0.5	0.0	0.0
		Perceived security (Lee et al., 2020)	Cheng et al. (2006), Lallmahamood (2007) and Oliveira, Thomas, Baptista, and Campos (2016)	1.0	1.0	1.0
		Perceived security (Aw et al., 2022)	Cheng et al. (2006)	0.5	1.0	1.0
		Perceived security (Lee, Sheehan et al., 2021)	Cheng et al. (2006)	1.0	1.0	1.0
Risk perception	29	Risk perception (Emami-Naeini et al., 2021)	Not reported	n.a.	n.a.	n.a.
		Perceived security risk (Shofolahan & Kang, 2018)	Hsu and Lin (2018)	1.0	1.0	1.0
		Perceived privacy risk (García de Blanes Sebastián et al., 2022)	Featherman and Pavlou (2003)	0.5	1.0	1.0
		Safety risk (Patil & Kulkarni, 2022)	Suplet, Gómez Suárez, and Díaz-Martín (2009)	1.0	1.0	1.0
		Perceived risk (Behera et al., 2021)	Trivedi (2019)	1.0	1.0	1.0
		Perceived privacy risk (McLean & Osei-Frimpong, 2019)	AlDebei2014 - Referenced paper not found	0.5	1.0	1.0
		Perceived privacy risk (Aiolfi, 2023)	McLean and Osei-Frimpong (2019)	1.0	1.0	1.0
		Perceived privacy risk (Vimalkumar et al., 2021)	Alalwan (2020), Bansal et al. (2016) and Smith et al. (2011, 1996)	1.0	1.0	1.0
		Perceived privacy risk (Kwangsawad & Jattamart, 2022)	Jattamart and Leelasantitham (2020) and Rese et al. (2020)	1.0	1.0	1.0
		Perceived privacy risk (Cha et al., 2021)	Kim, Park, Park, and Ahn (2019), Krasnova, Veltri, and Günther (2012) and Trepte, Scharkow, and Dienlin (2020)	1.0	1.0	1.0
		Security/Privacy risk (Kowalczuk, 2018)	Yang, Lee, and Zo (2017)	1.0	1.0	1.0
		Perceived risk (Kasilingam, 2020)	Featherman and Pavlou (2003)	1.0	1.0	1.0
		Perceived privacy risk (Pal, Roy et al., 2022)	Alalwan (2020) and Smith et al. (2011)	1.0	1.0	1.0
		Privacy risk (Guerreiro et al., 2022)	McLean and Osei-Frimpong (2019)	1.0	1.0	1.0
		Perceived privacy risk (Cheng & Jiang, 2020)	van Euwen (2017)	1.0	1.0	1.0
		Security/Privacy risk (Han & Yang, 2018)	Yang et al. (2017)	1.0	1.0	1.0
		Perceived risk (Hasan et al., 2021)	Zhou (2011)	1.0	1.0	1.0
		Perceived risk (Hsu & Lee, 2023)	Xu and Gupta (2009)	1.0	1.0	1.0
		Risk (Nordheim et al., 2019)	Corritore, Marble, Wiedenbeck, Kracher, and Chandran (2005)	0.5	1.0	0.0
		Privacy risk (Prakash et al., 2023)	Featherman and Pavlou (2003)	0.5	1.0	1.0
		Risk perception (Ahmad et al., 2022)	Colesca (2009) and Gulati et al. (2018)	0.0	0.0	0.0
		Perceived privacy risk (Kang & Oh, 2023)	Xu, Dinev, Smith and Hart (2011)	0.5	0.0	0.0
		Perceived personal data collection risk (Patrizi, Vernuccio, & Pastore, 2021)	McLean and Osei-Frimpong (2019)	1.0	0.0	0.0
		Perceived personal data misuse risk (Patrizi et al., 2021)	Dinev and Hart (2005)	1.0	0.0	0.0
		Privacy risk (Cao et al., 2022)	McLean and Osei-Frimpong (2019)	1.0	1.0	1.0
		Perceived privacy risk (Alt & Ibolya, 2021)	Yang, Liu, Li, and Yu (2015)	1.0	0.0	0.0
		Perceived privacy risk (Maroufkhani et al., 2022)	Yang et al. (2017)	1.0	1.0	1.0
		Perceived privacy risk (Jain et al., 2022)	Yang et al. (2017)	1.0	1.0	1.0
		Perceived privacy risk (Song, Du et al., 2022)	Song, Xing, Duan, Cohen and Mou (2022)	1.0	1.0	1.0

(*continued on next page*)

Table 16 (*continued*).

Construct	Frequency	Reference paper	Reference construct	Reliability testing	Convergent validity	Discriminant validity
Other related constructs	34	Privacy importance (Alghamdi et al., 2022)	Not reported	0.5	0.0	0.0
		Privacy preferences (Alghamdi et al., 2022)	Not reported	0.5	0.0	0.0
		Privacy preference (Ahmad et al., 2022)	Not reported	n.a.	n.a.	n.a.
		Privacy scores (Joy et al., 2022)	Not reported	n.a.	n.a.	n.a.
		Privacy self-efficacy (Ahmad et al., 2022)	Zeissig, Lidynia, Vervier, Gadeib, and Ziefle (2017)	0.5	0.0	0.0
		Privacy self-efficacy (Kang & Oh, 2023)	Chen (2018) and Krasnova, Spiekermann, Koroleva, and Hildebrand (2010)	0.5	0.0	0.0
		Privacy setting review (Xu et al., 2022)	Child et al. (2009), John (2022) and Norton (2018)	0.5	0.0	0.0
		Ownership protection (Xu et al., 2022)	Child et al. (2009), John (2022) and Norton (2018)	0.5	0.0	0.0
		Security and privacy behaviors (Shlega et al., 2022)	Haney, Furman, Theofanos, and Fahl (2019), Yao, Basdeo, Mcdonough, and Wang (2019) and Zeng, Mare, and Roesner (2017)	0.5	0.0	0.0
		Coping behavior (Park et al., 2021)	Son and Kim (2008)	1.0	1.0	1.0
		Trust in privacy (Cannizzaro, Procter, Ma, & Maple, 2020)	Not reported	1.0	1.0	1.0
		Trust in security (Cannizzaro et al., 2020)	Not reported	1.0	1.0	1.0
		Privacy awareness (Ahmad et al., 2022)	Zeissig et al. (2017)	0.5	0.0	0.0
		Privacy boundary linkage (Kang & Oh, 2023)	Child et al. (2009)	0.5	0.0	0.0
		Perceived protection of data (Shlega et al., 2022)	Not reported	0.5	0.0	0.0
		Threat to human identity (Uysal et al., 2022)	Ferrari, Paladino, and Jetten (2016) and Mende, Scott, van Doorn, Grewal, and Shanks (2019)	1.0	1.0	1.0
		IPA data confidence (Liao et al., 2019)	Not reported	0.5	0.0	0.0
		Data protection (Krey & Ramirez Garcia, 2022)	Not reported	n.a.	n.a.	n.a.
		Perceived level of comfort (Tabassum et al., 2019)	Not reported	n.a.	n.a.	n.a.
		Comfort level (Easwara Moorthy & Vu, 2015)	Not reported	n.a.	n.a.	n.a.
		Level of comfort with information disclosure (Ischen et al., 2020)	Croes and Antheunis (2021) and Ledbetter (2009)	0.5	0.0	0.0
		Security attitudes (Abdi et al., 2021)	Faklaris, Dabbish, and Hong (2019)	0.0	0.0	0.0
		Security attitudes (Abrokwa et al., 0000)	Faklaris et al. (2019)	0.5	0.0	0.0
		Security attitudes (Seymour, 2023)	Faklaris et al. (2019)	0.0	0.0	0.0
		Acceptability (Abdi et al., 2021)	Not reported	0.0	0.0	0.0
		Acceptability (Malkin et al., 2019)	Not reported	n.a.	n.a.	n.a.
		Creepiness (Dekkal et al., 2023)	Langer and König (2018)	0.5	1.0	1.0
		Recording sensitivity (Tabassum et al., 2019)	Not reported	n.a.	n.a.	n.a.
		Privacy cynicism (Acikgoz & Vega, 2022)	Choi, Park, and Jung (2018)	1.0	1.0	1.0
		Surveillance anxiety (Kowalczuk, 2018)	Kummer, Recker, and Bick (2017)	1.0	1.0	1.0
		Skepticism (Abrokwa et al., 0000)	Center (2019)	0.5	0.0	0.0
		Security and privacy knowledge (Abrokwa et al., 0000)	Center (2019)	0.5	0.0	0.0
		Perceived reliability (Ahmad et al., 2022)	Madsen and Gregor (2000)	0.0	0.0	0.0
		Perceived intrusiveness (Pal, Babakerkhell et al., 2022)	Lucia-Palacios and Pérez-López (2021)	1.0	1.0	1.0

Table 17
Overview of trust-related constructs used in mixed and quantitative studies. We display whether studies reused scales by showing the corresponding reference. We compute reliability and validity scores based on Rohan et al. (2023) as described in Section 5.2.3. "n.a" is used whenever studies did not rely on multi-item scales and thus, reliability and validity assessment was not possible.

Construct	Frequency	Reference paper	Reference construct	Reliability testing	Convergent validity	Discriminant validity
Trust	55	Trust in AIA (Uysal et al., 2022)	Leach, Ellemers, and Barreto (2007)	1.0	1.0	1.0
		Trust toward Alexa (Cho et al., 2020)	Koh and Sundar (2010)	0.5	0.0	0.0
		Trust (Seymour, 2023)	Cannizzaro et al. (2020)	0.0	0.0	0.0
		Trust (Ng et al., 2020)	Nordheim (2018)	0.5	0.0	0.0
		Trust (García de Blanes Sebastián et al., 2022)	Lu, Yang, Chau, and Cao (2011)	0.5	1.0	1.0
		Propensity to trust (Patil & Kulkarni, 2022)	Ashleigh, Higgs, and Dulewicz (2012), Li, Hess, and Valacich (2008), Mayer and Davis (1999) and McKnight, Choudhury, and Kacmar (2002)	1.0	1.0	1.0
		Perceived trust belief (Patil & Kulkarni, 2022)	Akter, D'Ambra, and Ray (2013)	1.0	1.0	1.0
		Perceived trust (Behera et al., 2021)	Kasilingam (2020)	1.0	1.0	1.0
		Trust (Dekkal et al., 2023)	Khalid, Shiung, Sheng, and Helander (2018)	0.5	1.0	1.0
		Trust (Vimalkumar et al., 2021)	Alalwan (2020), Bansal et al. (2016) and Smith et al. (2011, 1996)	1.0	1.0	1.0
		Trust (Acikgoz & Vega, 2022)	Kim et al. (2019)	1.0	1.0	1.0
		Trust (Pitardi & Marriott, 2021)	Chattaraman, Kwon, Gilbert, and Ross (2019), Hassanein and Head (2007) and Ye, Ying, Zhou, and Wang (2019)	1.0	1.0	1.0
		Trust (van Bussel et al., 2022)	Chandra, Srivastava, and Theng (2010)	1.0	0.5	1.0
		Trust (Fahn & Riener, 2021)	Davis (1993)	0.5	0.0	0.0
		TS-Trust (Fahn & Riener, 2021)	Jian et al. (2000)	0.5	0.0	0.0
		Mistrust (Fahn & Riener, 2021)	Jian et al. (2000)	0.5	0.0	0.0
		Trust (Kasilingam, 2020)	Chong, Chan, and Ooi (2012) and Tsu Wei, Marthandan, Yee-Loong Chong, Ooi, and Arumugam (2009)	1.0	1.0	1.0
		Trust (Pal, Roy et al., 2022)	Alalwan (2020) and Ye et al. (2019)	1.0	1.0	1.0
		Trust (Guerreiro et al., 2022)	Kääriä (2017)	1.0	1.0	1.0
		Trust (General after Mayer) (Cannizzaro et al., 2020)	Mayer et al. (1995)	0.0	0.0	0.0
		Trust (General after Mayer) (Bhattacherjee, 2002)	Mayer et al. (1995)	1.0	1.0	1.0
		Trust (General after Mayer) (Mari & Algesheimer, 2021)	Mayer et al. (1995)	0.5	0.0	0.0
		Trust (General) (Lin, Cronjé, Käthner, Pauli, & Latoschik, 2023)	Not reported (Yamagishi & Yamagishi, 1994)	n.a.	n.a.	n.a.
		Trust (General) (Hsu & Lee, 2023)	Dwyer, Hiltz, and Passerini (2007) and Metzger (2007)	1.0	1.0	1.0
		Trust (General) (Jiang et al., 2023)	Gefen, Karahanna, and Straub (2003)	1.0	1.0	1.0
		Trust (General) (Choung et al., 2023)	Schmidt, Biessmann, and Teubner (2020)	0.0	0.0	0.0
		Trust (General) (Lopez, Watkins, & Pak, 2023)	Lee and Moray (1992)	0.5	0.0	0.0
		Trust (General) (Hasan et al., 2021)	Kääriä (2017)	1.0	1.0	1.0
		Trust (General) (Moradinezhad & Solovey, 2021)	Jian et al. (2000)	0.0	0.0	0.0
		Trust (General) (Wald et al., 2021)	Bickmore and Cassell (2001)	0.0	0.0	0.0
		Trust (General) (Pitardi & Marriott, 2021)	Chattaraman et al. (2019) and Hassanein, Head, and Ju (2009)	1.0	1.0	1.0
		Trust (General) (Lee, Ayyagari, Nasirian and Ahmadian, 2021)	Kim, Mirusmonov, and Lee (2010) and Pham and Ho (2015)	0.5	1.0	1.0
		Trust (General) (Gupta et al., 2020)	Jian et al. (2000)	0.0	0.0	0.0
		Trust (General) (Toader et al., 2019)	Gupta, Yadav, and Varadarajan (2009)	1.0	1.0	1.0
		Perceived trust (Liu et al., 2021)	Kim et al. (2011) and Shuhaiber and Mashal (2019)	1.0	1.0	1.0
		Perceived trust (Pal et al., 2020)	Dinev et al. (2006) and Malhotra et al. (2004)	1.0	1.0	0.0
		Perceived trust (Purwanto et al., 2020)	Brill et al. (2022), Ejdys (2018) and Ejdys, Ginevicius, Rozsa, and Janoskova (2019)	1.0	1.0	1.0
		Perceived trust (Ahmad et al., 2022)	Jian et al. (2000)	0.0	0.0	0.0
		Perceived trust (Muñoz & Kremer, 2023)	Corritore, Kracher, and Wiedenbeck (2003)	0.5	0.0	0.0
		Brand trust (Lappeman et al., 2023)	Bruner, Hensel, and James (2005)	1.0	1.0	1.0
		Brand trust (Lv et al., 2022)	Nordheim (2018)	1.0	1.0	0.0
		Emotional trust (Lappeman et al., 2023)	Komiak and Benbasat (2006)	1.0	1.0	1.0
		Emotional trust (Pal, Babakerkhell et al., 2022)	Komiak and Benbasat (2006)	1.0	1.0	1.0

(*continued on next page*)

Table 17 (*continued*).

Construct	Frequency	Reference paper	Reference construct	Reliability testing	Convergent validity	Discriminant validity
		Emotional trust (Chen & Park, 2021)	Komiak and Benbasat (2006)	1.0	1.0	1.0
		Cognitive trust (Lappeman et al., 2023)	Not reported	1.0	1.0	1.0
		Cognitive trust (Pal, Babakerkhell et al., 2022)	Komiak and Benbasat (2006)	1.0	1.0	1.0
		Cognitive trust (Chen & Park, 2021)	Komiak and Benbasat (2006)	1.0	1.0	1.0
		Trusting intention (Kunkel et al., 2019)	Mcknight, Carter, Thatcher, and Clay (2011)	0.0	0.0	0.0
		Trusting intention (Prakash et al., 2023)	Lankton et al. (2015)	0.5	1.0	1.0
		Human-like trustworthiness (Weidmüller, 2022)	Lankton et al. (2015) and Mayer et al. (1995)	0.5	1.0	1.0
		Machine-like trustworthiness (Weidmüller, 2022)	Lankton et al. (2015) and Mayer et al. (1995)	0.5	1.0	1.0
		Institution-based trust (Kunkel et al., 2019)	McKnight et al. (2002)	0.0	0.0	0.0
		Disposition to trust (Kunkel et al., 2019)	McKnight et al. (2002)	0.0	0.0	0.0
		Perceived appropriateness trust (Casadei et al., 2022)	Davis (1989) and Nordheim et al. (2019)	n.a.	n.a.	n.a.
		Perceived trustworthiness (Tastemirova et al., 2022)	Ho and MacDorman (2010) and Latoschik et al. (2017)	0.5	0.0	0.0
Technology & trust	11	Human–computer trust (Pesonen, 2021)	Gulati, Sousa, and Lamas (2019)	0.5	0.0	0.0
		Trust in chatbots (Cyr, Head, Larios, & Pan, 2009)	Not reported	1.0	1.0	0.0
		Trust in chatbots (Everard & Galletta, 2005)	Not reported	n.a.	n.a.	n.a.
		Trust in chatbots (Alagarsamy & Mehrolia, 2023)	Not reported	1.0	1.0	1.0 .
		Trust in automation (Li, Erickson et al., 2023)	Jian et al. (2000)	0.0	0.0	0.0
		Trust in automation (Li, Kamaraj et al., 2023)	Jian et al. (2000)	n.a.	n.a.	n.a.
		Trust in automation (Merritt, Heimbaugh, LaChapell, & Lee, 2013)	Jian et al. (2000)	0.0	0.0	0.0
		Trust in automation (Weitz, Schiller, Schlagowski, Huber, & André, 2019)	Jian et al. (2000)	0	0	0
		Trust in AI (Salah, Alhalbusi, Ismail, & Abdelfattah, 2023)	Gulati et al. (2019)	1.0	1.0	1.0
		Trust in technology (Lv et al., 2022)		1.0	1.0	0.0
		System trust scale (Gupta et al., 2019)	Jian et al. (2000)	n.a.	n.a.	n.a.
Trust (Mayer)	25	Benevolence (Goodman & Mayhorn, 2023)	Elkins and Derrick (2013), Harwood and Garry (2017) and Mcknight et al. (2011)	1.0	1.0	1.0
		Benevolence (Weidmüller, 2022)	Elkins and Derrick (2013), Harwood and Garry (2017) and Mcknight et al. (2011)	0.5	1.0	1.0
		Benevolence (Hu et al., 2021)	Elkins and Derrick (2013), Harwood and Garry (2017) and Mcknight et al. (2011)	1.0	1.0	1.0
		Benevolence (Mari & Algesheimer, 2021)	Elkins and Derrick (2013), Harwood and Garry (2017) and Mcknight et al. (2011)	0.5	0.0	0.0
		Benevolence (Gulati et al., 2018)	Elkins and Derrick (2013), Harwood and Garry (2017) and Mcknight et al. (2011)	1.0	1.0	1.0
		Integrity (Lappeman et al., 2023)	Elkins and Derrick (2013)	1.0	1.0	1.0
		Integrity (Weidmüller, 2022)	Elkins and Derrick (2013)	0.5	1.0	1.0
		Integrity (Goodman & Mayhorn, 2023)	Elkins and Derrick (2013)	1.0	1.0	1.0
		Integrity (Hu et al., 2021)	Elkins and Derrick (2013)	1.0	1.0	1.0
		Integrity (Mari & Algesheimer, 2021)	Elkins and Derrick (2013)	0.5	0.0	0.0
		Trust belief (Prakash et al., 2023)	Lankton et al. (2015)	0.5	1.0	1.0
		Trust belief (Jiang et al., 2023)	Lankton et al. (2015)	1.0	1.0	1.0
		Trust belief (Kunkel et al., 2019)	Lankton et al. (2015)	0.0	0.0	0.0
		Competence (Lappeman et al., 2023)	McKnight et al. (2002) and Skjuve and Brandzaeg (2019)	1.0	1.0	1.0
		Competence (Weidmüller, 2022)	McKnight et al. (2002) and Skjuve and Brandzaeg (2019)	0.5	1.0	1.0
		Competence (Wald et al., 2021)	McKnight et al. (2002) and Skjuve and Brandzaeg (2019)	0.0	0.0	0.0
		Competence (Hu et al., 2021)	McKnight et al. (2002) and Skjuve and Brandzaeg (2019)	1.0	1.0	1.0
		Competence (Mari & Algesheimer, 2021)	McKnight et al. (2002) and Skjuve and Brandzaeg (2019)	0.5	0.0	0.0
		Competence (Gulati et al., 2018)	McKnight et al. (2002) and Skjuve and Brandzaeg (2019)	1.0	1.0	1.0
		Technical competence (Lee & Sun, 2022)	Madsen and Gregor (2000)	0.0	1.0	0.0
		Chatbot competence	Cho (2006)	1.0	1.0	1.0
		Chatbot competence	Holzwarth, Janiszewski, and Neumann (2006)	0.5	0.0	1.0
		Perceived task solving competence	Erskine, Khojah, and McDaniel (2019)	1.0	1.0	1.0
		Perceived task solving competence	Aaker, Vohs, and Mogilner (2010) and Fiske, Cuddy, Glick, and Xu (2018)	0.0	0.0	0.0

(*continued on next page*)

Table 17 (*continued*).

Construct	Frequency	Reference paper	Reference construct	Reliability testing	Convergent validity	Discriminant validity
		Perceived performance (Purwanto et al., 2020)	Davis (1989), Kim, Ferrin, and Rao (2008), Malhotra et al. (2004) and Xiao and Benbasat (2002)	1.0	1.0	1.0
		Professionalism (Lv et al., 2022)	Nordheim (2018)	1.0	1.0	0.0
		Ability (Goodman & Mayhorn, 2023)	Elkins and Derrick (2013)	1.0	1.0	1.0
		Perceived benefits (Pal et al., 2020)		1.0	1.0	0.0
		Reputation (Nordheim et al., 2019)	Corritore et al. (2005)	n.a.	n.a.	n.a.
Other constructs related to trust	13	Reliability (Lee & Sun, 2022)	Lankton et al. (2015) and Madsen and Gregor (2000)	0.0	1.0	0.0
		Reliability (Weidmüller, 2022)	Lankton et al. (2015) and Madsen and Gregor (2000)	0.5	1.0	1.0
		Understandability (Lee & Sun, 2022)		0.0	1.0	0.0
		Previous chatbot usage (Jiang et al., 2023)		1.0	1.0	1.0
		Previous chatbot usage (Wald et al., 2021)		0.0	0.0	0.0
		Tailored response (Jiang et al., 2023)	Schuetzler, Grimes, and Scott Giboney (2020)	1.0	1.0	1.0
		Communication delay	Schanke, Burtch, and Ray (2021)	0.0	0.0	0.0
		Communication delay	Liu and Gal (2011)	0.0	0.0	0.0
		Communal relationship (Cheng et al., 2022)	Li, Chan, and Kim (2019) and Wang, Mao, Li, and Liu (2017)	1.0	1.0	1.0
Interactivity	3	Synchronicity (Purwanto et al., 2020)	Brill et al. (2022)	1.0	1.0	1.0
		Bidirectionality (Purwanto et al., 2020)	Brill et al. (2022) and Yoo, Lee, and Park (2010)	1.0	1.0	1.0
		Perceived interactivity (Prakash et al., 2023)	Go and Sundar (2019)	0.5	1.0	1.0
Affect, Humanness, Anthropomorphism	29	Voice humanness (Hu et al., 2021)	Go and Sundar (2019)	1.0	1.0	1.0
		Understanding humanness (Hu et al., 2021)	Go and Sundar (2019)	1.0	1.0	1.0
		Affinity for technology (Gupta, Basu, Ghantasala, Qiu, & Gadiraju, 2022)	Franke, Attig, and Wessel (2019)	0.0	0.0	0.0
		Perceived warmth (Cheng et al., 2022)	Kirmani, Hamilton, Thompson, and Lantzy (2017)	1.0	1.0	1.0
		Virtual assistant warmth (Toader et al., 2019)	Aaker et al. (2010)	1.0	1.0	1.0
		Perceived humanity (Zhang et al., 2021)	Venkatesh and Davis (2000)	1.0	1.0	0.0
		Perceived social presence (Zhang et al., 2021)	Venkatesh and Davis (2000)	1.0	1.0	0.0
		Perceived social interactivity (Zhang et al., 2021)	Venkatesh and Davis (2000)	1.0	1.0	0.0
		Anthropomorphism (Chen & Park, 2021)	Bartneck, Kulić, Croft, and Zoghbi (2009) and Waytz, Cacioppo, and Epley (2010)	1.0	1.0	1.0
		Anthropomorphism (Wald et al., 2021)	Bartneck et al. (2009) and Waytz et al. (2010)	0.0	0.0	0.0
		Anthropomorphic design cues (Toader et al., 2019)	Nowak and Rauh (2005)	1.0	1.0	1.0
		Social Presence (Lee & Sun, 2022)	Biocca, Harms, and Burgoon (2003), Bruwer, Emsley, Kidd, Lochner, and Seedat (2008), Gefen et al. (2003), Gray (1977) and King and He (2006)	0.0	1.0	0.0
		Social Presence (Kunkel et al., 2019)	Biocca et al. (2003), Bruwer et al. (2008), Gefen et al. (2003), Gray (1977) and King and He (2006)	0.0	0.0	0.0
		Social Presence (Prakash et al., 2023)	Biocca et al. (2003), Bruwer et al. (2008), Gefen et al. (2003), Gray (1977) and King and He (2006)	0.5	1.0	1.0
		Social Presence (Jiang et al., 2023)	Biocca et al. (2003), Bruwer et al. (2008), Gefen et al. (2003), Gray (1977) and King and He (2006)	1.0	1.0	1.0
		Social Presence (Pitardi & Marriott, 2021)	Biocca et al. (2003), Bruwer et al. (2008), Gefen et al. (2003), Gray (1977) and King and He (2006)	1.0	1.0	1.0
		Social Presence (Toader et al., 2019)	Biocca et al. (2003), Bruwer et al. (2008), Gefen et al. (2003), Gray (1977) and King and He (2006)	1.0	1.0	1.0
		Social Cognition (Pitardi & Marriott, 2021)	Fiske and Macrae (2012)	1.0	1.0	1.0
		Interpersonal attraction (Chen & Park, 2021)	Han and Yang (2018)	1.0	1.0	1.0
		Humanlike traits (Hsu & Lee, 2023)	Lewis and Hardzinski (2015)	1.0	1.0	1.0
		Humanlike cues (Li & Sung, 2021)		0	0	
		Humanlikeness (Lv et al., 2022)	Ho and MacDorman (2010)	1.0	1.0	0
		Humanlikeness (Weidmüller, 2022)	Ho and MacDorman (2010)	0.5	1.0	1.0
		Humanlikeness (Nordheim et al., 2019)	Ho and MacDorman (2010)	n.a.	n.a.	n.a.
		Helpfulness (Weidmüller, 2022)	Lankton et al. (2015)	0.5	1.0	1.0
		Faith (Lee & Sun, 2022)	Madsen and Gregor (2000)	0	1.0	0.0
		Personal attachment (Lee & Sun, 2022)	Madsen and Gregor (2000)	0.0	1.0	0.0
		Familiarity (Liu et al., 2021)		1.0	1.0	1.0

(*continued on next page*)

Table 17 (*continued*).

Construct	Frequency	Reference paper	Reference construct	Reliability testing	Convergent validity	Discriminant validity
Character & personality	15	Self-esteem (Salah et al., 2023)	Gnambs, Scharl, and Schroeders (2018)	1.0	1.0	1.0
		Disposition to trust (Alagarsamy & Mehrolia, 2023)	Tan and Sutherland (2005)	1.0	1.0	1.0
		Propensity to trust technology (Prakash et al., 2023)	Lankton et al. (2015) and Mayer et al. (1995)	0.5	1.0	1.0
		Psychological well-being (Salah et al., 2023)	Babnik, Benko, and von Humboldt (2022)	1.0	1.0	1.0
		Personality (Lv et al., 2022)	Not reported	1.0	1.0	0.0
		Conformity (Schreuter, van der Putten, & Lamers, 2021)	Mehrabian and Stefl (1995)	0.0	0.0	0.0
		Ambiguity tolerance (Jiang et al., 2023)	Budner (1962)	1.0	1.0	1.0
		Technology optimism (Liu et al., 2021)	Shuhaiber and Mashal (2019)	1.0	1.0	1.0
		Extraversion (Müller et al., 2019)	Wang and Benbasat (2016)	0.5	0.0	0.0
		Agreeableness (Müller et al., 2019)	Wang and Benbasat (2016)	0.5	0.0	0.0
		Emotionality (Müller et al., 2019)	Wang and Benbasat (2016)	0.5	0.0	0
		Honesty–humility (Müller et al., 2019)	Wang and Benbasat (2016)	0.5	0.0	0.0
		Honesty (Gulati et al., 2018)	McKnight et al. (2002)	1.0	1.0	1.0
		Social disclosure (Toader et al., 2019)	Cho (2006)	1.0	1.0	1.0
Other constructs	13	Personalized services (Pal et al., 2020)	Xu, Luo, Carroll and Rosson (2011)	1.0	1.0	1.0
		Follow advice (Kunkel et al., 2019)	Not reported	n.a.	n.a.	n.a.
		Follow advice (Lin et al., 2023)	Not reported	n.a.	n.a.	n.a.
		Give information (Kunkel et al., 2019)	Not reported	0.0	0.0	0.0
		Job anxiety (Salah et al., 2023)	Wang and Wang (2022)	1.0	1.0	1.0
		Reciprocity (Gulati et al., 2018)	Kankanhalli, Tan, and Wei (2005)	1.0	1.0	1.0
		Technology fear (Alagarsamy & Mehrolia, 2023)	Cabrera-Sánchez, Villarejo-Ramos, Liébana-Cabanillas, and Shaikh (2021)	1.0	1.0	1.0
		Decision satisfaction (Mari & Algesheimer, 2021)	Fitzsimons (2000) and Fitzsimons, Greenleaf, and Lehmann (1997)	0.5	0.0	0.0
		Ubiquity (Compeau & Higgins, 1995)		1.0	1.0	1.0
		Positive consumer response (Toader et al., 2019)	Cyr, Bonanni, and Ilsever (2004)	1.0	1.0	1.0
		Perceived stereotyping (Salah et al., 2023)	Schepman and Rodway (2023)	1.0	1.0	1.0
		Perceived contingency (Prakash et al., 2023)	Go and Sundar (2019)	0.5	1.0	1.0
		Perceived complementary (Pal et al., 2020)	Lee and Lee (2014)	1.0	1.0	0.0

Table 18
Research methods in our sample.

Research method	Privacy & security - Frequency (Percentage)	Trust - Frequency (Percentage)
Quantitative	60 (60%)	47 (81%)
Survey	45 (45%)	22 (38%)
Experiment and survey	12 (12%)	11 (19%)
Vignette study	3 (3%)	14 (24%)
Trust game	–	2 (3%)
Mixed	19 (19%)	6 (10%)
Experiment and survey and interview	5 (5%)	
Interview and survey	3 (3%)	2 (3%)
Focus group and survey	2 (2%)	
Survey and analysis of posted reviews	2 (2%)	
Experiment and interview and focus group and observation	1 (1%)	
Experiment and interview and datalogs and drawing	1 (1%)	
Experiment and survey and card sorting	1 (1%)	
Experiment and mixed survey	1 (1%)	3 (5%)
Experience sampling method and survey	1 (1%)	
Delphi study and survey	1 (1%)	
Design science research and interview and survey	1 (1%)	
Mixed survey		1 (2%)
Qualitative	21 (21%)	5 (9%)
Interview	15 (15%)	3 (5%)
Focus group	1 (1%)	
Interview and focus group	1 (1%)	
Interview and diary study	1 (1%)	
Interview and datalogs	1 (1%)	
Interview and drawing	1 (1%)	
Focus group and co-design	1 (1%)	
Interview with coding		1 (2%)
Collaborative design		1 (2%)

References

Aaker, J., Vohs, K. D., & Mogilner, C. (2010). Nonprofits are seen as warm and for-profits as competent: Firm stereotypes matter. *Journal of Consumer Research*, *37*(2), 224–237.

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* (pp. 1–14). Yokohama Japan: ACM, http://dx.doi.org/10.1145/3411764.3445122.

Abrokwa, D., Das, S., Akgul, O., & Mazurek, M. L. Comparing security and privacy attitudes among U.S. users of different smartphone and smart-speaker platforms.

Acikgoz, F., & Vega, R. P. (2022). The role of privacy cynicism in consumer habits with voice assistants: A technology acceptance model perspective. *International Journal of Human–Computer Interaction*, *38*(12), 1138–1152. http://dx.doi.org/10.1080/10447318.2021.1987677.

Ackerman, M. S. (2004). Privacy in pervasive environments: next generation labeling protocols. *Personal and Ubiquitous Computing*, *8*(6), 430–439. http://dx.doi.org/10.1007/s00779-004-0305-8.

Ahmad, I., Akter, T., Buher, Z., Farzan, R., Kapadia, A., & Lee, A. J. (2022). Tangible privacy for smart voice assistants: Bystanders' perceptions of physical device controls. *Proceedings of the ACM on Human-Computer Interaction*, *6*(CSCW2), 1–31. http://dx.doi.org/10.1145/3555089.

Ahmad, I., Farzan, R., Kapadia, A., & Lee, A. J. (2020). Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proceedings of the ACM on Human-Computer Interaction*, *4*(CSCW2), 1–28. http://dx.doi.org/10.1145/3415187.

Aiolfi, S. (2023). How shopping habits change with artificial intelligence: Smart speakers' usage intention. *International Journal of Retail & Distribution Management*, *ahead-of-print*(ahead-of-print), http://dx.doi.org/10.1108/IJRDM-11-2022-0441.

Akter, S., D'Ambra, J., & Ray, P. (2013). Development and validation of an instrument to measure user perceived service quality of mHealth. *Information & Management*, *50*(4), 181–195. http://dx.doi.org/10.1016/j.im.2013.03.001.

Al-Ameen, M. N., Chauhan, A., Ahsan, M. M., & Kocabas, H. (2021). A look into user's privacy perceptions and data practices of IoT devices. *Information & Computer Security*, *29*(4), 573–588. http://dx.doi.org/10.1108/ICS-08-2020-0134.

Alagarsamy, S., & Mehrolia, S. (2023). Exploring chatbot trust: Antecedents and behavioural outcomes. *Heliyon*, *9*(5).

Alalwan, A. A. (2020). Mobile food ordering apps: An empirical study of the factors affecting customer e-satisfaction and continued intention to reuse. *International Journal of Information Management*, *50*, 28–44. http://dx.doi.org/10.1016/j.ijinfomgt.2019.04.008.

Alghamdi, L., Alsoubai, A., Akter, M., Alghamdi, F., & Wisniewski, P. (2022). A user study to evaluate a web-based prototype for smart home internet of things device management. In *International conference on human-computer interaction* (pp. 383–405). Springer, http://dx.doi.org/10.1007/978-3-031-05563-8_24.

Alt, M.-A., & Ibolya, V. (2021). Identifying relevant segments of potential banking chatbot users based on technology adoption behavior. *Market-Tržište*, *33*(2), 165–183.

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*, *26*(3), 1–28. http://dx.doi.org/10.1145/3311956.

Ashleigh, M. J., Higgs, M., & Dulewicz, V. (2012). A new propensity to trust scale and its relationship with individual well-being: Implications for HRM policies and practices. *Human Resource Management Journal*, *22*(4), 360–376. http://dx.doi.org/10.1111/1748-8583.12007.

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*, Article 121711.

Ayalon, O., & Toch, E. (2019). Evaluating {users'} perceptions about a {system's} privacy: Differentiating social and institutional aspects. In *Fifteenth symposium on usable privacy and security* (pp. 41–59).

Babnik, K., Benko, E., & von Humboldt, S. (2022). Ryff's psychological well-being scale. In *Encyclopedia of gerontology and population aging* (pp. 4344–4349). Springer.

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. http://dx.doi.org/10.1016/j.im.2015.08.001.

Bar-Ilan, J. (2018). Tale of three databases: The implication of coverage demonstrated for a sample query. *Frontiers in Research Metrics and Analytics*, *3*.

Barkhuus, L. (2012). The mismeasurement of privacy: Using contextual integrity to reconsider privacy in HCI. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 367–376). New York, NY, USA: Association for Computing Machinery, http://dx.doi.org/10.1145/2207676.2207727.

Bartneck, C., Kulić, D., Croft, E., & Zoghbi, S. (2009). Measurement instruments for the anthropomorphism, animacy, likeability, perceived intelligence, and perceived safety of robots. *International Journal of Social Robotics*, *1*, 71–81.

Bauer, P. C., & Freitag, M. (2018). Measuring trust. *The Oxford Handbook of Social and Political Trust*, *15*.

Behera, R. K., Bala, P. K., & Ray, A. (2021). Cognitive chatbot for personalised contextual customer service: Behind the scene and beyond the hype. *Information Systems Frontiers*, http://dx.doi.org/10.1007/s10796-021-10168-y.

Berg, J., Dickhaut, J., & McCabe, K. (1995). Trust, reciprocity, and social history. *Games and Economic Behavior*, *10*(1), 122–142.

Bhattacherjee, A. (2002). Individual trust in online firms: Scale development and initial test. *Journal of Management Information Systems*, *19*(1), 211–241.

Bickmore, T., & Cassell, J. (2001). Relational agents: a model and implementation of building user trust. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 396–403).

Biocca, F., Harms, C., & Burgoon, J. K. (2003). Toward a more robust theory and measure of social presence: Review and suggested criteria. *Presence: Teleoperators & Virtual Environments*, *12*(5), 456–480.

Bolton, T., Dargahi, T., Belguith, S., Al-Rakhami, M. S., & Sodhro, A. H. (2021). On the security and privacy challenges of virtual assistants. *Sensors*, *21*(7), 2312. http://dx.doi.org/10.3390/s21072312.

Borsci, S., Malizia, A., Schmettow, M., van der Velde, F., Tariverdiyeva, G., Balaji, D., et al. (2022). The chatbot usability scale: The design and pilot of a usability scale for interaction with AI-based conversational agents. *Personal and Ubiquitous Computing*, *26*(1), 95–119. http://dx.doi.org/10.1007/s00779-021-01582-9.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, *4*(3), 340–347. http://dx.doi.org/10.1177/1948550612455931, Publisher: SAGE Publications Inc.

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.

Brüggemeier, B., & Lalone, P. (2022). Perceptions and reactions to conversational privacy initiated by a conversational user interface. *Computer Speech and Language*, *71*, Article 101269. http://dx.doi.org/10.1016/j.csl.2021.101269.

Bruner, G. C., Hensel, P. J., & James, K. E. (2005). *Marketing scales handbook*. American Marketing Association Chicago, IL.

Bruwer, B., Emsley, R., Kidd, M., Lochner, C., & Seedat, S. (2008). Psychometric properties of the multidimensional scale of perceived social support in youth. *Comprehensive Psychiatry*, *49*(2), 195–201.

Budner, S. (1962). Intolerance of ambiguity as a personality variable. *Journal of Personality Assessment*, (1), 29–50.

Buteau, E., & Lee, J. (2021). Hey Alexa, why do we use voice assistants? The driving factors of voice assistant technology use. *Communication Research Reports*, *38*(5), 336–345. http://dx.doi.org/10.1080/08824096.2021.1980380.

Cabrera-Sánchez, J.-P., Villarejo-Ramos, Á. F., Liébana-Cabanillas, F., & Shaikh, A. A. (2021). Identifying relevant segments of AI applications adopters–Expanding the UTAUT2's variables. *Telematics and Informatics*, *58*, Article 101529.

Cannizzaro, S., Procter, R., Ma, S., & Maple, C. (2020). Trust in the smart home: Findings from a nationally representative survey in the UK. *PLoS One*, *15*(5), Article e0231615.

Cao, D., Sun, Y., Goh, E., Wang, R., & Kuiavska, K. (2022). Adoption of smart voice assistants technology among Airbnb guests: a revised self-efficacy-based value adoption model (SVAM). *International Journal of Hospitality Management*, *101*, Article 103124.

Carlos Roca, J., José García, J., & José De La Vega, J. (2009). The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security*, *17*(2), 96–113. http://dx.doi.org/10.1108/09685220910963983.

Casadei, A., Schlögl, S., & Bergmann, M. (2022). Chatbots for robotic process automation: Investigating perceived trust and user satisfaction. In *2022 IEEE 3rd international conference on human-machine systems* (pp. 1–6). IEEE.

Casaló, L. V., Flavián, C., & Guinalíu, M. (2007). The role of security, privacy, usability and reputation in the development of online banking. *Online Information Review*, *31*(5), 583–603. http://dx.doi.org/10.1108/14684520710832315.

Center, P. R. (2019). American trends panel wave 49. [Online] https://www.pewresearch.org/internet/dataset/american-trends-panel-wave-49/.

Cha, H. S., Wi, J. H., Park, C., & Kim, T. (2021). Sustainability calculus in adopting smart speakers—personalized services and privacy risks. *Sustainability*, *13*(2), 602. http://dx.doi.org/10.3390/su13020602.

Chandra, S., Srivastava, S. C., & Theng, Y.-L. (2010). Evaluating the role of trust in consumer adoption of mobile payment systems: An empirical analysis. *Communications of the Association for Information Systems*, *27*, http://dx.doi.org/10.17705/1CAIS.02729.

Chattaraman, V., Kwon, W.-S., Gilbert, J. E., & Ross, K. (2019). Should AI-based, conversational digital assistants employ social-or task-oriented interaction style? A task-competency and reciprocity perspective for older adults. *Computers in Human Behavior*, *90*, 315–330.

Chen, H.-T. (2018). Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. *American Behavioral Scientist*, *62*(10), 1392–1412.

Chen, Q. Q., & Park, H. J. (2021). How anthropomorphism affects trust in intelligent personal assistants. *Industrial Management & Data Systems*, *121*(12), 2722–2737.

Cheng, Y., & Jiang, H. (2020). How do AI-driven chatbots impact user experience? Examining gratifications, perceived privacy risk, satisfaction, loyalty, and continued use. *Journal of Broadcasting & Electronic Media*, *64*(4), 592–614. http://dx.doi.org/10.1080/08838151.2020.1834296.

Cheng, T. C. E., Lam, D. Y. C., & Yeung, A. C. L. (2006). Adoption of internet banking: An empirical study in Hong Kong. *Decision Support Systems*, *42*(3), 1558–1572. http://dx.doi.org/10.1016/j.dss.2006.01.002.

Cheng, X., Zhang, X., Cohen, J., & Mou, J. (2022). Human vs. AI: Understanding the impact of anthropomorphism on consumer response to chatbots from the perspective of trust and relationship norms. *Information Processing & Management*, *59*(3), Article 102940.

Child, J. T., Pearson, J. C., & Petronio, S. (2009). Blogging, communication, and privacy management: Development of the blogging privacy management measure. *Journal of the American Society for Information Science and Technology*, *60*(10), 2079–2094. http://dx.doi.org/10.1002/asi.21122.

Chita-Tegmark, M., Law, T., Rabb, N., & Scheutz, M. (2021). Can you trust your trust measure? In *Proceedings of the 2021 ACM/IEEE international conference on human-robot interaction* (pp. 92–100).

Cho, J. (2006). The mechanism of trust and distrust formation and their relational outcomes. *Journal of Retailing*, *82*(1), 25–35.

Cho, E. (2019). Hey google, can I ask you something in private? In *Proceedings of the 2019 CHI conference on human factors in computing systems* (pp. 1–9). Glasgow Scotland Uk: ACM, http://dx.doi.org/10.1145/3290605.3300488.

Cho, E., Sundar, S. S., Abdullah, S., & Motalebi, N. (2020). Will deleting history make alexa more trustworthy?: Effects of privacy and content customization on user experience of smart speakers. In *Proceedings of the 2020 CHI conference on human factors in computing systems* (pp. 1–13). Honolulu HI USA: ACM, http://dx.doi.org/10.1145/3313831.3376551.

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

Choi, Y. K., Thompson, H. J., & Demiris, G. (2020). Use of an internet-of-things smart home system for healthy aging in older adults in residential settings: Pilot feasibility study. *JMIR Aging*, *3*(2), Article e21964. http://dx.doi.org/10.2196/21964.

Choi, S., & Zhou, J. (2023). Inducing consumers' self-disclosure through the fit between chatbot's interaction styles and regulatory focus. *Journal of Business Research*, *166*, Article 114127.

Chong, A. Y.-L., Chan, F. T. S., & Ooi, K.-B. (2012). Predicting consumer decisions to adopt mobile commerce: Cross country empirical examination between China and Malaysia. *Decision Support Systems*, *53*(1), 34–43. http://dx.doi.org/10.1016/j.dss.2011.12.001.

Choung, H., David, P., & Ross, A. (2023). Trust in AI and its role in the acceptance of AI technologies. *International Journal of Human–Computer Interaction*, *39*(9), 1727–1739.

Colesca, S. E. (2009). Understanding trust in e-government. *Engineering Economics*, *63*(3).

Colnago, J., Cranor, L. F., Acquisti, A., & Stanton, K. H. (2022). Is it a concern or a preference? An investigation into the ability of privacy scales to capture and distinguish granular privacy constructs. In *Eighteenth symposium on usable privacy and security* (pp. 331–346). Boston, MA: USENIX Association, URL: https://www.usenix.org/conference/soups2022/presentation/colnago.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, 189–211.

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: concepts, evolving themes, a model. *International Journal of Human-Computer Studies*, *58*(6), 737–758.

Corritore, C. L., Marble, R. P., Wiedenbeck, S., Kracher, B., & Chandran, A. (2005). Measuring online trust of websites: Credibility, perceived ease of use, and risk. In *AMCIS 2005 proceedings*.

Cowan, B. R., Pantidi, N., Coyle, D., Morrissey, K., Clarke, P., Al-Shehri, S., et al. (2017). "What can i help you with?": Infrequent users' experiences of intelligent personal assistants. In *mobileHCI '17*, *Proceedings of the 19th international conference on human-computer interaction with mobile devices and services* (pp. 1–12). New York, NY, USA: Association for Computing Machinery, http://dx.doi.org/10.1145/3098279.3098539.

Croes, E. A., & Antheunis, M. L. (2021). Can we be friends with mitsuku? A longitudinal study on the process of relationship formation between humans and a social chatbot. *Journal of Social and Personal Relationships*, *38*(1), 279–300.

Culnan, M., & Williams, C. (2009). How ethics can enhance organizational privacy: Lessons from the ChoicePoint and TJX data breaches. *MIS Quarterly*, *33*(4), 673–687, URL: https://aisel.aisnet.org/misq/vol33/iss4/6.

Cyr, D., Bonanni, C., & Ilsever, J. (2004). Design and e-loyalty across cultures in electronic commerce. In *Proceedings of the 6th international conference on electronic commerce* (pp. 351–360).

Cyr, D., Head, M., Larios, H., & Pan, B. (2009). Exploring human images in website design: a multi-method approach. *MIS Quarterly*, 539–566.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319–340.

Davis, F. D. (1993). User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *International Journal of Man-Machine Studies*, *38*(3), 475–487. http://dx.doi.org/10.1006/imms.1993.1022.

de Barcelos Silva, A., Gomes, M. M., da Costa, C. A., da Rosa Righi, R., Barbosa, J. L. V., Pessin, G., et al. (2020). Intelligent personal assistants: A systematic literature review. *Expert Systems with Applications*, *147*, Article 113193. http://dx.doi.org/10.1016/j.eswa.2020.113193.

De Graaf, M. M., Ben Allouch, S., & van Dijk, J. A. (2016). Long-term evaluation of a social robot in real homes. *Interaction Studies*, *17*(3), 462–491.

Dekkal, M., Arcand, M., Prom Tep, S., Rajaobelina, L., & Ricard, L. (2023). Factors affecting user trust and intention in adopting chatbots: The moderating role of technology anxiety in insurtech. *Journal of Financial Services Marketing*, http://dx.doi.org/10.1057/s41264-023-00230-y.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce–a study of Italy and the United States. *European Journal of Information Systems*, *15*(4), 389–402.

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, *10*(2), 7–29. http://dx.doi.org/10.2753/JEC1086-4415100201.

Distler, V., Fassl, M., Habib, H., Krombholz, K., Lenzini, G., Lallemand, C., et al. (2021). A systematic literature review of empirical methods and risk representation in usable privacy and security research. *ACM Transactions on Computer-Human Interaction*, *28*(6), 1–50. http://dx.doi.org/10.1145/3469845.

Durall Gazulla, E., Martins, L., & Fernández-Ferrer, M. (2023). Designing learning technology collaboratively: Analysis of a chatbot co-design. *Education and Information Technologies*, *28*(1), 109–134.

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of facebook and myspace. In *AMCIS 2007 proceedings* (p. 339).

Dzindolet, M. T., Peterson, S. A., Pomranky, R. A., Pierce, L. G., & Beck, H. P. (2003). The role of trust in automation reliance. *International Journal of Human-Computer Studies*, *58*(6), 697–718.

Easwara Moorthy, A., & Vu, K.-P. L. (2015). Privacy concerns for use of voice activated personal assistant in the public space. *International Journal of Human-Computer Interaction*, *31*(4), 307–335.

Edu, J. S., Such, J. M., & Suarez-Tangil, G. (2021). Smart home personal assistants: A security and privacy review. *ACM Computing Surveys*, *53*(6), 1–36. http://dx.doi.org/10.1145/3412383, arXiv:1903.05593.

Ejdys, J. (2018). Building technology trust in ICT application at a university. *International Journal of Emerging Markets*, *13*(5), 980–997.

Ejdys, J., Ginevicius, R., Rozsa, Z., & Janoskova, K. (2019). The role of perceived risk and security level in building trust in E-government solutions. *E+M Ekonomie a Management*, *22*(3), 220–235.

Elkins, A. C., & Derrick, D. C. (2013). The sound of trust: voice as a measurement of trust during interactions with embodied conversational agents. *Group Decision and Negotiation*, *22*(5), 897–913.

Emami-Naeini, P., Dheenadhayalan, J., Agarwal, Y., & Cranor, L. F. (2021). Which privacy and security attributes most impact consumers' risk perception and willingness to purchase IoT devices? In *2021 IEEE symposium on security and privacy* (pp. 519–536). http://dx.doi.org/10.1109/SP40001.2021.00112.

Erskine, M. A., Khojah, M., & McDaniel, A. E. (2019). Location selection using heat maps: Relative advantage, task-technology fit, and decision-making performance. *Computers in Human Behavior*, *101*, 151–162.

Everard, A., & Galletta, D. F. (2005). How presentation flaws affect perceived site quality, trust, and intention to purchase from an online store. *Journal of Management Information Systems*, *22*(3), 56–95.

Fahn, V., & Riener, A. (2021). Time to get conversational: Assessment of the potential of conversational user interfaces for mobile banking. In *Mensch und computer 2021* (pp. 34–43). Ingolstadt Germany: ACM, http://dx.doi.org/10.1145/3473856.3473872.

Fakhimi, A., Garry, T., & Biggemann, S. (2023). The effects of anthropomorphised virtual conversational assistants on consumer engagement and trust during service encounters. *Australasian Marketing Journal*, Article 14413582231181140.

Faklaris, C., Dabbish, L. A., & Hong, J. I. (2019). A {self-report} measure of {end-user} security attitudes ({{{{{sa-6}}}}}). In *Fifteenth symposium on usable privacy and security* (pp. 61–77).

Faqih, K. M. S., & Jaradat, M.-I. R. M. (2015). Assessing the moderating effect of gender differences and individualism-collectivism at individual-level on the adoption of mobile commerce technology: TAM3 perspective. *Journal of Retailing and Consumer Services*, *22*, 37–52. http://dx.doi.org/10.1016/j.jretconser.2014.09.006.

Farooq, A., Jeske, D., van Schaik, P., & Moran, M. (2022). Voice assistants:(physical) device use perceptions, acceptance, and privacy concerns. In *Conference on e-business, e-services and e-society* (pp. 485–498). Springer.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: a perceived risk facets perspective. *International Journal of Human-Computer Studies*, *59*(4), 451–474.

Fernaeus, Y., Håkansson, M., Jacobsson, M., & Ljungblad, S. (2010). How do you play with a robotic toy animal? A long-term study of pleo. In *Proceedings of the 9th international conference on interaction design and children* (pp. 39–48).

Ferrari, F., Paladino, M., & Jetten, J. (2016). Blurring human–machine distinctions: Anthropomorphic appearance in social robots as a threat to human distinctiveness. *International Journal of Social Robotics*, *8*, http://dx.doi.org/10.1007/s12369-016-0338-y.

Fiske, S. T., Cuddy, A. J., Glick, P., & Xu, J. (2018). A model of (often mixed) stereotype content: Competence and warmth respectively follow from perceived status and competition. In *Social cognition* (pp. 162–214). Routledge.

Fiske, S. T., & Macrae, C. N. (2012). *The SAGE handbook of social cognition*. Sage.

Fitzsimons, G. J. (2000). Consumer response to stockouts. *Journal of Consumer Research*, *27*(2), 249–266.

Fitzsimons, G. J., Greenleaf, E. A., & Lehmann, D. R. (1997). Decision and consumption satisfaction: Implications for channel relations. *Marketing Studies Center Working Paper Series*, *313*.

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. http://dx.doi.org/10.1108/02635570610666403.

Franke, T., Attig, C., & Wessel, D. (2019). A personal resource for technology interaction: development and validation of the affinity for technology interaction (ATI) scale. *International Journal of Human–Computer Interaction*, *35*(6), 456–467.

Furini, M., Mirri, S., Montangero, M., & Prandi, C. (2020). On the usage of smart speakers during the Covid-19 coronavirus lockdown. In *Proceedings of the 6th EAI international conference on smart objects and technologies for social good* (pp. 187–192). Antwerp Belgium: ACM, http://dx.doi.org/10.1145/3411170.3411260.

García de Blanes Sebastián, M., Sarmiento Guede, J. R., & Antonovica, A. (2022). Application and extension of the UTAUT2 model for determining behavioral intention factors in use of the artificial intelligence virtual assistants. *Frontiers in Psychology*, *13*.

Gauder, L., Pepino, L., Riera, P., Brussino, S., Vidal, J., Gravano, A., et al. (2023). Towards detecting the level of trust in the skills of a virtual assistant from the user's speech. *Computer Speech and Language*, *80*, Article 101487.

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

Gnambs, T., Scharl, A., & Schroeders, U. (2018). The structure of the rosenberg self-esteem scale. *Zeitschrift für Psychologie*.

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

Goodman, K. L., & Mayhorn, C. B. (2023). It's not what you say but how you say it: Examining the influence of perceived voice assistant gender and pitch on trust and reliance. *Applied Ergonomics*, *106*, Article 103864.

Gray, G. (1977). In J. Short, E. Williams, & B. Christie (Eds.), *The social psychology of telecommunications* (p. 195). London, New York, Sydney, Toronto: John Wiley and Sons, 1976.

Gross, T. (2021). Validity and reliability of the scale internet users' information privacy concerns (IUIPC). *Vol. 2021*, In *Proceedings on privacy enhancing technologies* (pp. 235–258).

Guerreiro, J., Loureiro, S. M. C., & Ribeiro, C. (2022). Advertising acceptance via smart speakers. *Spanish Journal of Marketing - ESIC*, *26*(3), 286–308. http://dx.doi.org/10.1108/SJME-02-2022-0028.

Gulati, S., Sousa, S., & Lamas, D. (2018). Modelling trust in human-like technologies. In *Proceedings of the 9th Indian conference on human-computer interaction* (pp. 1–10).

Gulati, S., Sousa, S., & Lamas, D. (2019). Design, development and evaluation of a human-computer trust scale. *Behaviour & Information Technology*, *38*(10), 1004–1015.

Gupta, A., Basu, D., Ghantasala, R., Qiu, S., & Gadiraju, U. (2022). To trust or not to trust: How a conversational interface affects trust in a decision support system. In *Proceedings of the ACM web conference 2022* (pp. 3531–3540).

Gupta, K., Hajika, R., Pai, Y. S., Duenser, A., Lochner, M., & Billinghurst, M. (2019). In ai we trust: Investigating the relationship between biosignals, trust and cognitive load in vr. In *Proceedings of the 25th ACM symposium on virtual reality software and technology* (pp. 1–10).

Gupta, K., Hajika, R., Pai, Y. S., Duenser, A., Lochner, M., & Billinghurst, M. (2020). Measuring human trust in a virtual assistant using physiological sensing in virtual reality. In *2020 IEEE conference on virtual reality and 3D user interfaces* (pp. 756–765). IEEE.

Gupta, P., Yadav, M. S., & Varadarajan, R. (2009). How task-facilitative interactive tools foster buyers' trust in online retailers: a process view of trust development in the electronic marketplace. *Journal of Retailing*, *85*(2), 159–176.

Gusenbauer, M., & Haddaway, N. (2020). Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of google scholar, PubMed and 26 other resources [open access]. *Research Synthesis Methods*, *11*, 181–217. http://dx.doi.org/10.1002/jrsm.1378.

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.

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). *Classroom companion: business*, *Partial least squares structural equation modeling (PLS-SEM) using R: A workbook*. Cham: Springer International Publishing, http://dx.doi.org/10.1007/978-3-030-80519-7.

Han, S., & Yang, H. (2018). Understanding adoption of intelligent personal assistants: A parasocial relationship perspective. *Industrial Management & Data Systems*, *118*(3), 618–636. http://dx.doi.org/10.1108/IMDS-05-2017-0214.

Haney, J., Furman, S. M., Theofanos, M., & Fahl, Y. A. (2019). Perceptions of smart home privacy and security responsibility, concerns, and mitigations.

Harkous, H., Fawaz, K., Shin, K. G., & Aberer, K. (2016). {PriBots}: Conversational privacy with chatbots. In *Twelfth symposium on usable privacy and security*.

Harwood, T., & Garry, T. (2017). Internet of things: understanding trust in techno-service systems. *Journal of Service Management*, *28*(3), 442–475.

Hasan, R., Shams, R., & Rahman, M. (2021). Consumer trust and perceived risk for voice-controlled artificial intelligence: The case of Siri. *Journal of Business Research*, *131*, 591–597. http://dx.doi.org/10.1016/j.jbusres.2020.12.012.

Hassanein, K., & Head, M. (2007). Manipulating perceived social presence through the web interface and its impact on attitude towards online shopping. *International Journal of Human-Computer Studies*, *65*(8), 689–708. http://dx.doi.org/10.1016/j.ijhcs.2006.11.018.

Hassanein, K., Head, M., & Ju, C. (2009). A cross-cultural comparison of the impact of social presence on website trust, usefulness and enjoyment. *International Journal of Electronic Business*, *7*(6), 625–641.

Hinds, P. J. (1998). *User control and its many facets: A study of perceived control in human-computer interaction*. Hewlett Packard Laboratories California.

Ho, C.-C., & MacDorman, K. F. (2010). Revisiting the uncanny valley theory: Developing and validating an alternative to the Godspeed indices. *Computers in Human Behavior*, *26*(6), 1508–1518.

Hoff, K. A., & Bashir, M. (2015). Trust in automation: Integrating empirical evidence on factors that influence trust. *Human Factors*, *57*(3), 407–434.

Holzwarth, M., Janiszewski, C., & Neumann, M. M. (2006). The influence of avatars on online consumer shopping behavior. *Journal of Marketing*, *70*(4), 19–36.

Hornung, O., & Smolnik, S. (2022). AI invading the workplace: Negative emotions towards the organizational use of personal virtual assistants. *Electronic Markets*, *32*(1), 123–138. http://dx.doi.org/10.1007/s12525-021-00493-0.

Hsu, W.-C., & Lee, M.-H. (2023). Semantic technology and anthropomorphism: Exploring the impacts of voice assistant personality on user trust, perceived risk, and attitude. *Journal of Global Information Management (JGIM)*, *31*(1), 1–21.

Hsu, C.-L., & Lin, J. C.-C. (2018). Exploring factors affecting the adoption of internet of things services. *Journal of Computer Information Systems*, *58*(1), 49–57. http://dx.doi.org/10.1080/08874417.2016.1186524.

Hu, P., Lu, Y., et al. (2021). Dual humanness and trust in conversational AI: A person-centered approach. *Computers in Human Behavior*, *119*, Article 106727.

Ischen, C., Araujo, T., Voorveld, H., Van Noort, G., & Smit, E. (2020). Privacy concerns in chatbot interactions. In A. Følstad, T. Araujo, S. Papadopoulos, E. L.-C. Law, O.-C. Granmo, E. Luger, & P. B. Brandtzaeg (Eds.), *Chatbot research and design*: *vol. 11970*, (pp. 34–48). Cham: Springer International Publishing, http://dx.doi.org/10.1007/978-3-030-39540-7_3.

Ivarsson, J., & Lindwall, O. (2023). Suspicious minds: the problem of trust and conversational agents. *Computer Supported Cooperative Work (CSCW)*, 1–27.

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.

Jameel, A. S., & Karem, M. A. (2022). Perceived trust and enjoyment: Predicting behavioural intention to use mobile payment systems. In *2022 international conference on intelligent technology, system and service for internet of everything* (pp. 1–6). IEEE.

Jattamart, A., & Leelasantitham, A. (2020). Perspectives to social media usage of depressed patients and caregivers affecting to change the health behavior of patients in terms of information and perceived privacy risks. *Heliyon*, *6*(6), Article e04244. http://dx.doi.org/10.1016/j.heliyon.2020.e04244.

Jian, J.-Y., Bisantz, A. M., & Drury, C. G. (2000). Foundations for an empirically determined scale of trust in automated systems. *International Journal of Cognitive Ergonomics*, *4*(1), 53–71. http://dx.doi.org/10.1207/S15327566IJCE0401_04.

Jiang, Y., Yang, X., & Zheng, T. (2023). Make chatbots more adaptive: Dual pathways linking human-like cues and tailored response to trust in interactions with chatbots. *Computers in Human Behavior*, *138*, Article 107485.

John, A. S. (2022). How to set up a smart speaker for privacy. https://www.consumerreports.org/electronics-computers/privacy/smart-speaker-privacy-settings-a8054333211/. (Accessed Online 13 December 2023).

Joy, D., Kotevska, O., & Al-Masri, E. (2022). Investigating users' privacy concerns of internet of things (IoT) smart devices. In *2022 IEEE 4th eurasia conference on IOT, communication and engineering* (pp. 70–76). http://dx.doi.org/10.1109/ECICE55674.2022.10042926.

Kääriä, A. (2017). *Technology acceptance of voice assistants: anthropomorphism as factor* (Master's thesis), University of Jyväskylä.

Kaddour, J., Harris, J., Mozes, M., Bradley, H., Raileanu, R., & McHardy, R. (2023). Challenges and applications of large language models. arXiv preprint arXiv:2307.10169.

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.

Kankanhalli, A., Tan, B. C., & Wei, K.-K. (2005). Contributing knowledge to electronic knowledge repositories: An empirical investigation. *MIS Quarterly*, 113–143.

Kasilingam, D. L. (2020). Understanding the attitude and intention to use smartphone chatbots for shopping. *Technology in Society*, *62*, Article 101280. http://dx.doi.org/10.1016/j.techsoc.2020.101280.

Kefi, H., Besson, E., Sokolova, K., & Aouina-Mejri, C. (2021). Privacy and intelligent virtual assistants usage across generations. *Systèmes d'Information et Management*, *26*(2), 43–76.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163–1173.

Khalid, H. M., Shiung, L. W., Sheng, V. B., & Helander, M. G. (2018). Trust of virtual agent in multi actor interactions. *Journal of Robotics, Networking and Artificial Life*, *4*(4), 295–298. http://dx.doi.org/10.2991/jrnal.2018.4.4.8.

Kim, M.-J., Chung, N., & Lee, C.-K. (2011). The effect of perceived trust on electronic commerce: Shopping online for tourism products and services in South Korea. *Tourism Management*, *32*(2), 256–265.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, *44*(2), 544–564.

Kim, C., Mirusmonov, M., & Lee, I. (2010). An empirical examination of factors influencing the intention to use mobile payment. *Computers in Human Behavior*, *26*(3), 310–322.

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. http://dx.doi.org/10.1016/j.chb.2018.11.022.

King, W. R., & He, J. (2006). A meta-analysis of the technology acceptance model. *Information & Management*, *43*(6), 740–755.

Kirmani, A., Hamilton, R. W., Thompson, D. V., & Lantzy, S. (2017). Doing well versus doing good: The differential effect of underdog positioning on moral and competent service providers. *Journal of Marketing*, *81*(1), 103–117.

Kitkowska, A., Karegar, F., & Wästlund, E. (2023). Share or protect: Understanding the interplay of trust, privacy concerns, and data sharing purposes in health and well-being apps. In *Proceedings of the 15th biannual conference of the Italian SIGCHI chapter* (pp. 1–14). Torino Italy: ACM, http://dx.doi.org/10.1145/3605390.3605417.

Koh, Y. J., & Sundar, S. S. (2010). Effects of specialization in computers, web sites, and web agents on e-commerce trust. *International Journal of Human-Computer Studies*, *68*(12), 899–912. http://dx.doi.org/10.1016/j.ijhcs.2010.08.002.

Komiak, S. Y., & Benbasat, I. (2006). The effects of personalization and familiarity on trust and adoption of recommendation agents. *MIS Quarterly*, 941–960.

König, C. M., Karrenbauer, C., & Breitner, M. H. (2023). Critical success factors and challenges for individual digital study assistants in higher education: A mixed methods analysis. *Education and Information Technologies*, *28*(4), 4475–4503. http://dx.doi.org/10.1007/s10639-022-11394-w.

Kosa, T. A. (2010). Vampire bats: Trust in privacy. In *2010 eighth international conference on privacy, security and trust* (pp. 96–102). IEEE.

Kowalczuk, P. (2018). Consumer acceptance of smart speakers: A mixed methods approach. *Journal of Research in Interactive Marketing*, *12*(4), 418–431. http://dx.doi.org/10.1108/JRIM-01-2018-0022.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, *25*(2), 109–125.

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering*, *4*(3), 127–135. http://dx.doi.org/10.1007/s12599-012-0216-6.

Krey, M., & Ramirez Garcia, R. (2022). Voice assistants in healthcare: The patient's perception. In *2022 8th international conference on information management* (pp. 120–130). http://dx.doi.org/10.1109/ICIM56520.2022.00029.

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

Kunkel, J., Donkers, T., Michael, L., Barbu, C.-M., & Ziegler, J. (2019). Let me explain: Impact of personal and impersonal explanations on trust in recommender systems. In *Proceedings of the 2019 CHI conference on human factors in computing systems* (pp. 1–12).

Kwangsawad, A., & Jattamart, A. (2022). Overcoming customer innovation resistance to the sustainable adoption of chatbot services: A community-enterprise perspective in Thailand. *Journal of Innovation & Knowledge*, *7*(3), Article 100211. http://dx.doi.org/10.1016/j.jik.2022.100211.

Lallmahamood, M. (2007). An examination of individuals perceived security and privacy of the internet in Malaysia and the influence ofthis on their intention to use E-commerce: Using AnExtension of the technology acceptance model. *The Journal of Internet Banking and Commerce*, *12*, 1–26, URL: https://api.semanticscholar.org/CorpusID:167934491.

Langer, M., & König, C. J. (2018). Introducing and testing the creepiness of situation scale (CRoSS). *Frontiers in Psychology*, *9*.

Lankton, N. K., McKnight, D. H., & Tripp, J. (2015). Technology, humanness, and trust: Rethinking trust in technology. *Journal of the Association for Information Systems*, *16*(10), 1.

Lappeman, J., Marlie, S., Johnson, T., & Poggenpoel, S. (2023). Trust and digital privacy: Willingness to disclose personal information to banking chatbot services. *Journal of Financial Services Marketing*, *28*(2), 337–357. http://dx.doi.org/10.1057/s41264-022-00154-z.

Latoschik, M. E., Roth, D., Gall, D., Achenbach, J., Waltemate, T., & Botsch, M. (2017). The effect of avatar realism in immersive social virtual realities. In *Proceedings of the 23rd ACM symposium on virtual reality software and technology* (pp. 1–10).

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. http://dx.doi.org/10.1145/3274371.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–42. http://dx.doi.org/10.1111/j.1540-4560.1977.tb01880.x.

Lazar, J., Feng, J. H., & Hochheiser, H. (2017). *Research methods in human-computer interaction*. Morgan Kaufmann.

Leach, C. W., Ellemers, N., & Barreto, M. (2007). Group virtue: The importance of morality (vs. Competence and sociability) in the positive evaluation of in-groups. *Journal of Personality and Social Psychology*, *93*(2), 234–249. http://dx.doi.org/10.1037/0022-3514.93.2.234.

Ledbetter, A. M. (2009). Measuring online communication attitude: Instrument development and validation. *Communication Monographs*, *76*(4), 463–486.

Lee, K., & Ashton, M. C. (2004). Psychometric properties of the HEXACO personality inventory. *Multivariate Behavioral Research*, *39*(2), 329–358.

Lee, O.-K. D., Ayyagari, R., Nasirian, F., & Ahmadian, M. (2021). Role of interaction quality and trust in use of AI-based voice-assistant systems. *Journal of Systems and Information Technology*, *23*(2), 154–170.

Lee, M., Frank, L., & IJsselsteijn, W. (2021). Brokerbot: A cryptocurrency chatbot in the social-technical gap of trust. *Computer Supported Cooperative Work (CSCW)*, *30*(1), 79–117. http://dx.doi.org/10.1007/s10606-021-09392-6.

Lee, J., Kim, J., & Choi, J. Y. (2019). The adoption of virtual reality devices: The technology acceptance model integrating enjoyment, social interaction, and strength of the social ties. *Telematics and Informatics*, *39*, 37–48.

Lee, S., & Lee, S. (2014). Early diffusion of smartphones in OECD and BRICS countries: An examination of the effects of platform competition and indirect network effects. *Telematics and Informatics*, *31*(3), 345–355.

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*(3), 563–583. http://dx.doi.org/10.1007/s10796-019-09975-1.

Lee, J., & Moray, N. (1992). Trust, control strategies and allocation of function in human-machine systems. *Ergonomics*, *35*(10), 1243–1270.

Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors*, *46*(1), 50–80.

Lee, K. Y., Sheehan, L., Lee, K., & Chang, Y. (2021). The continuation and recommendation intention of artificial intelligence-based voice assistant systems (AIVAS): the influence of personal traits. *Internet Research*, *31*(5), 1899–1939.

Lee, S. K., & Sun, J. (2022). Testing a theoretical model of trust in human-machine communication: emotional experience and social presence. *Behaviour & Information Technology*, 1–14.

Lewis, J. R., & Hardzinski, M. L. (2015). Investigating the psychometric properties of the speech user interface service quality questionnaire. *International Journal of Speech Technology*, *18*, 479–487.

Li, X., Chan, K. W., & Kim, S. (2019). Service with emoticons: How customers interpret employee use of emoticons in online service encounters. *Journal of Consumer Research*, *45*(5), 973–987.

Li, M., Erickson, I. M., Cross, E. V., & Lee, J. D. (2023). It's not only what you say, but also how you say it: Machine learning approach to estimate trust from conversation. *Human Factors*, Article 00187208231166624.

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. http://dx.doi.org/10.1016/j.jsis.2008.01.001.

Li, M., Kamaraj, A. V., & Lee, J. D. (2023). Modeling trust dimensions and dynamics in human-agent conversation: A trajectory epistemic network analysis approach. *International Journal of Human–Computer Interaction*, 1–12.

Li, X., & Sung, Y. (2021). Anthropomorphism brings us closer: The mediating role of psychological distance in user–AI assistant interactions. *Computers in Human Behavior*, *118*, Article 106680.

Liao, Y., Vitak, J., Kumar, P., Zimmer, M., & Kritikos, K. (2019). Understanding the role of privacy and trust in intelligent personal assistant adoption. In N. G. Taylor, C. Christian-Lamb, M. H. Martin, & B. Nardi (Eds.), *Information in contemporary society*: *vol. 11420*, (pp. 102–113). Cham: Springer International Publishing, http://dx.doi.org/10.1007/978-3-030-15742-5_9.

Lim, N. (2003). Consumers' perceived risk: sources versus consequences. *Electronic Commerce Research and Applications*, *2*(3), 216–228. http://dx.doi.org/10.1016/S1567-4223(03)00025-5, URL: https://www.sciencedirect.com/science/article/pii/S1567422303000255. Selected Papers from the Pacific Asia Conference on Information Systems.

Lin, J., Cronjé, J., Käthner, I., Pauli, P., & Latoschik, M. E. (2023). Measuring interpersonal trust towards virtual humans with a virtual maze paradigm. *IEEE Transactions on Visualization and Computer Graphics*, *29*(5), 2401–2411.

Lin, V. Z., & Parkin, S. (2020). Transferability of privacy-related behaviours to shared smart home assistant devices. In *2020 7th international conference on internet of things: systems, management and security* (pp. 1–8). http://dx.doi.org/10.1109/IOTSMS52051.2020.9340199.

Liu, W., & Gal, D. (2011). Bringing us together or driving us apart: The effect of soliciting consumer input on consumers' propensity to transact with an organization. *Journal of Consumer Research*, *38*(2), 242–259.

Liu, Y., Gan, Y., Song, Y., & Liu, J. (2021). What influences the perceived trust of a voice-enabled smart home system: an empirical study. *Sensors*, *21*(6), 2037.

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. http://dx.doi.org/10.1016/j.im.2004.01.003.

Lopez, J., Watkins, H., & Pak, R. (2023). Enhancing component-specific trust with consumer automated systems through humanness design. *Ergonomics*, *66*(2), 291–302.

Lu, Y., Yang, S., Chau, P. Y., & Cao, Y. (2011). Dynamics between the trust transfer process and intention to use mobile payment services: A cross-environment perspective. *Information & Management*, *48*(8), 393–403.

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*(1), 41–54.

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

Lv, Y., Hu, S., Liu, F., & Qi, J. (2022). Research on users' trust in customer service chatbots based on human-computer interaction. In *China national conference on big data and social computing* (pp. 291–306). Springer.

Maccario, G., & Naldi, M. (2023). Privacy in smart speakers: A systematic literature review. *Security and Privacy*, *6*(1), Article e274. http://dx.doi.org/10.1002/spy2.274.

Madsen, M., & Gregor, S. (2000). Measuring human-computer trust. *Vol. 53*, In *11th Australasian conference on information systems* (pp. 6–8). Citeseer.

Malhotra, N., Kim, S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*, 336–355. http://dx.doi.org/10.1287/isre.1040.0032.

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

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*, 32–44.

Manikonda, L., Deotale, A., & Kambhampati, S. (2018). 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* (pp. 229–235). New Orleans LA USA: ACM, http://dx.doi.org/10.1145/3278721.3278773.

Maqableh, M., Hmoud, H. Y., Jaradat, M., et al. (2021). Integrating an information systems success model with perceived privacy, perceived security, and trust: the moderating role of facebook addiction. *Heliyon*, *7*(9).

Marangunić, N., & Granić, A. (2015). Technology acceptance model: a literature review from 1986 to 2013. *Universal Access in the Information Society*, *14*, 81–95.

Mari, A., & Algesheimer, R. (2021). The role of trusting beliefs in voice assistants during voice shopping. In *Hawaii International Conference on System Sciences 2021*.

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*, Article 121870.

Masur, P. K. (2019). *Situational privacy and self-disclosure*. Cham: Springer International Publishing, http://dx.doi.org/10.1007/978-3-319-78884-5.

Mayer, R. C., & Davis, J. H. (1999). The effect of the performance appraisal system on trust for management: A field quasi-experiment. *Journal of Applied Psychology*, *84*(1), 123–136. http://dx.doi.org/10.1037/0021-9010.84.1.123.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*(3), 709–734.

McCarthy, A., Gaster, B. R., & Legg, P. (2020). Shouting through letterboxes: A study on attack susceptibility of voice assistants. In *2020 international conference on cyber security and protection of digital services* (pp. 1–8). Dublin, Ireland: IEEE, http://dx.doi.org/10.1109/CyberSecurity49315.2020.9138860.

Mcknight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems (TMIS)*, *2*(2), 1–25.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: a trust building model. *The Journal of Strategic Information Systems*, *11*(3–4), 297–323.

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. http://dx.doi.org/10.1016/j.chb.2019.05.009.

Mehrabian, A., & Stefl, C. A. (1995). Basic temperament components of loneliness, shyness, and conformity. *Social Behavior and Personality: an International Journal*, *23*(3), 253–263.

Mende, M., Scott, M. L., van Doorn, J., Grewal, D., & Shanks, I. (2019). Service robots rising: How humanoid robots influence service experiences and elicit compensatory consumer responses. *Journal of Marketing Research*, *56*(4), 535–556. http://dx.doi.org/10.1177/0022243718822827.

Merritt, S. M., Heimbaugh, H., LaChapell, J., & Lee, D. (2013). I trust it, but I don't know why: Effects of implicit attitudes toward automation on trust in an automated system. *Human Factors*, *55*(3), 520–534.

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication*, *9*(4), JCMC942. http://dx.doi.org/10.1111/j.1083-6101.2004.tb00292.x.

Metzger, M. J. (2007). Making sense of credibility on the web: Models for evaluating online information and recommendations for future research. *Journal of the American Society for Information Science and Technology*, *58*(13), 2078–2091.

Mhaidli, A., Venkatesh, M. K., Zou, Y., & Schaub, F. (2020). Listen only when spoken to: Interpersonal communication cues as smart speaker privacy controls. *Proceedings on Privacy Enhancing Technologies*, *2020*(2), 251–270. http://dx.doi.org/10.2478/popets-2020-0026.

Misiolek, N. I., Zakaria, N., & Zhang, P. (2002). Trust in organizational acceptance of information technology: A conceptual model and preliminary evidence. In *33rd annual meeting of the decision sciences institute*.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & Group, T. P. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *PLoS Medicine*, *6*(7), Article e1000097. http://dx.doi.org/10.1371/journal.pmed.1000097.

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. http://dx.doi.org/10.1177/13548565211042234.

Moradinezhad, R., & Solovey, E. T. (2021). Investigating trust in interaction with inconsistent embodied virtual agents. *International Journal of Social Robotics*, *13*(8), 2103–2118.

Müller, L., Mattke, J., Maier, C., Weitzel, T., & Graser, H. (2019). Chatbot acceptance: A latent profile analysis on individuals' trust in conversational agents. In *Proceedings of the 2019 on computers and people research conference* (pp. 35–42).

Muñoz, N., & Kremer, B. A. (2023). The voice era: Future acceptance of digital voice assistants and how they will transform consumers' online purchasing behaviour. *Applied Marketing Analytics*, *8*(3), 255–270.

Ng, M., Coopamootoo, K. P., Toreini, E., Aitken, M., Elliot, K., & van Moorsel, A. (2020). Simulating the effects of social presence on trust, privacy concerns & usage intentions in automated bots for finance. In *2020 IEEE European symposium on security and privacy workshops* (pp. 190–199). http://dx.doi.org/10.1109/EuroSPW51379.2020.00034.

Nissenbaum, H. (2009). *Stanford law books*, *Privacy in context: technology, policy, and the integrity of social life*. Stanford University Press, URL: https://books.google.de/books?id=_NN1uGn1Jd8C.

Nordheim, C. B. (2018). *Trust in chatbots for customer service–findings from a questionnaire study* (Master's thesis), University of Oslo.

Nordheim, C. B., Følstad, A., & Bjørkli, C. A. (2019). An initial model of trust in chatbots for customer service—findings from a questionnaire study. *Interacting with Computers*, *31*(3), 317–335.

Norton (2018). Can smart speakers be hacked? 10 tips to help stay secure. https://us.norton.com/blog/iot/can-smart-speakers-be-hacked. (Accessed Online 13 December 2023).

Nowak, K. L., & Rauh, C. (2005). The influence of the avatar on online perceptions of anthropomorphism, androgyny, credibility, homophily, and attraction. *Journal of Computer-Mediated Communication*, *11*(1), 153–178.

Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2016). Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. *Computers in Human Behavior*, *61*, 404–414. http://dx.doi.org/10.1016/j.chb.2016.03.030.

Pal, D., Arpnikanondt, C., & Razzaque, M. A. (2020). Personal information disclosure via voice assistants: the personalization–privacy paradox. *SN Computer Science*, *1*, 1–17.

Pal, D., Babakerkhell, M. D., & Roy, P. (2022). How perceptions of trust and intrusiveness affect the adoption of voice activated personal assistants. *IEEE Access*, *10*, 123094–123113.

Pal, D., Roy, P., Arpnikanondt, C., & Thapliyal, H. (2022). The effect of trust and its antecedents towards determining users' behavioral intention with voice-based consumer electronic devices. *Heliyon*, *8*(4), Article e09271. http://dx.doi.org/10.1016/j.heliyon.2022.e09271.

Panjaitan, A. G., & Utomo, R. G. (2023). The influence of users' perception of security, privacy, and trust in using online dating applications. In *2023 11th international conference on information and communication technology* (pp. 551–556). IEEE.

Park, J., Choi, H., & Jung, Y. (2021). Users' cognitive and affective response to the risk to privacy from a smart speaker. *International Journal of Human–Computer Interaction*, *37*(8), 759–771.

Patil, K., & Kulkarni, M. (2022). Can we trust health and wellness chatbot going mobile? Empirical research using TAM and HBM. In *2022 IEEE region 10 symposium* (pp. 1–6). http://dx.doi.org/10.1109/TENSYMP54529.2022.9864368.

Patrizi, M., Vernuccio, M., & Pastore, A. (2021). Talking to voice assistants: Exploring negative and positive users' perceptions. In *Digital marketing & eCommerce conference* (pp. 24–34). Springer.

Pattnaik, N., Li, S., & Nurse, J. R. C. (2023). A survey of user perspectives on security and privacy in a home networking environment. *ACM Computing Surveys*, *55*(9), 1–38. http://dx.doi.org/10.1145/3558095.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, *7*(3), 101–134.

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research*, *15*(1), 37–59.

Perez Garcia, M., & Saffon Lopez, S. (2018). Building trust between users and telecommunications data driven virtual assistants. In *IFIP international conference on artificial intelligence applications and innovations* (pp. 628–637). Springer.

Pesonen, J. A. (2021). 'Are you OK?' students' trust in a chatbot providing support opportunities. In *International conference on human-computer interaction* (pp. 199–215). Springer.

Pettersson, I., Lachner, F., Frison, A.-K., Riener, A., & Butz, A. (2018). A bermuda triangle? A review of method application and triangulation in user experience evaluation. In *Proceedings of the 2018 CHI conference on human factors in computing systems* (pp. 1–16). New York, NY, USA: Association for Computing Machinery, http://dx.doi.org/10.1145/3173574.3174035.

Pham, T.-T. T., & Ho, J. C. (2015). The effects of product-related, personal-related factors and attractiveness of alternatives on consumer adoption of NFC-based mobile payments. *Technology in Society*, *43*, 159–172.

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.

Prakash, A. V., Joshi, A., Nim, S., & Das, S. (2023). Determinants and consequences of trust in AI-based customer service chatbots. *The Service Industries Journal*, *43*(9–10), 642–675.

Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies*, *71*(12), 1133–1143. http://dx.doi.org/10.1016/j.ijhcs.2013.09.002.

Purwanto, P., Kuswandi, K., & Fatmah, F. (2020). Interactive applications with artificial intelligence: The role of trust among digital assistant users. *Foresight and STI Governance*, *14*(2), 64–75, URL: https://foresight-journal.hse.ru/en/2020-14-2/370913009.html.

Quinn, K. (2016). Why we share: A uses and gratifications approach to privacy regulation in social media use. *Journal of Broadcasting & Electronic Media*, *60*(1), 61–86.

Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021). Human factors in cybersecurity: A scoping review. In *The 12th international conference on advances in information technology* (pp. 1–11). Bangkok Thailand: ACM, http://dx.doi.org/10.1145/3468784.3468789.

Rajapaksha, S., Thakrar, S., Kinzler, M., Sun, H., Smith, J., & Perouli, D. (2021). Field study on usability and security perceptions surrounding social robots. In *2021 IEEE 45th annual computers, software, and applications conference* (pp. 1593–1598). http://dx.doi.org/10.1109/COMPSAC51774.2021.00237.

Rauschnabel, P. A., Rossmann, A., & tom Dieck, M. C. (2017). An adoption framework for mobile augmented reality games: The case of Pokémon Go. *Computers in Human Behavior*, *76*, 276–286.

Renz, A., Neff, T., Baldauf, M., & Maier, E. (2023). Authentication methods for voice services on smart speakers – a multi-method study on perceived security and ease of use. *i-com*, *22*(1), 67–81. http://dx.doi.org/10.1515/icom-2022-0039.

Rese, A., Ganster, L., & Baier, D. (2020). Chatbots in retailers' customer communication: How to measure their acceptance? *Journal of Retailing and Consumer Services*, *56*, Article 102176. http://dx.doi.org/10.1016/j.jretconser.2020.102176.

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon*, *9*(3), Article e14234. http://dx.doi.org/10.1016/j.heliyon.2023.e14234.

Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality*.

Saffarizadeh, K., Boodraj, M., Alashoor, T. M., et al. (2017). Conversational assistants: Investigating privacy concerns, trust, and self-disclosure. In *ICIS*.

Salah, M., Alhalbusi, H., Ismail, M. M., & Abdelfattah, F. (2023). Chatting with ChatGPT: Decoding the mind of chatbot users and unveiling the intricate connections between user perception, trust and stereotype perception on self-esteem and psychological well-being. *Research Square*, 1–26.

Salisbury, W. D., Pearson, R. A., Pearson, A. W., & Miller, D. W. (2001). Perceived security and World Wide Web purchase intention. *Industrial Management & Data Systems*, *101*(4), 165–177. http://dx.doi.org/10.1108/02635570110390071.

Schanke, S., Burtch, G., & Ray, G. (2021). Estimating the impact of "humanizing" customer service chatbots. *Information Systems Research*, *32*(3), 736–751.

Schepman, A., & Rodway, P. (2023). The general attitudes towards artificial intelligence scale (GAAIS): Confirmatory validation and associations with personality, corporate distrust, and general trust. *International Journal of Human–Computer Interaction*, *39*(13), 2724–2741.

Schmidt, P., Biessmann, F., & Teubner, T. (2020). Transparency and trust in artificial intelligence systems. *Journal of Decision Systems*, *29*(4), 260–278.

Schomakers, E.-M., Biermann, H., & Ziefle, M. (2021). Users' Preferences for Smart Home Automation – Investigating Aspects of Privacy and Trust. *Telematics and Informatics*, *64*, Article 101689. http://dx.doi.org/10.1016/j.tele.2021.101689.

Schomakers, E.-M., Lidynia, C., & Ziefle, M. (2022). The role of privacy in the acceptance of smart technologies: Applying the privacy calculus to technology acceptance. *International Journal of Human–Computer Interaction*, *38*(13), 1276–1289.

Schrepp, M., & Thomaschewski, J. (2019). Design and validation of a framework for the creation of user experience questionnaires. *International Journal of Interactive Multimedia and Artificial Intelligence*, *5*(7), 88–95. http://dx.doi.org/10.9781/ijimai.2019.06.006, URL: https://www.ijimai.org/journal/sites/default/files/files/2019/06/ijimai20195_7_9_pdf_19082.pdf.

Schreuter, D., van der Putten, P., & Lamers, M. H. (2021). Trust me on this one: conforming to conversational assistants. *Minds and Machines*, *31*, 535–562.

Schuetzler, R. M., Grimes, G. M., & Scott Giboney, J. (2020). The impact of chatbot conversational skill on engagement and perceived humanness. *Journal of Management Information Systems*, *37*(3), 875–900.

Seymour, W. (2023). Ignorance is bliss? The effect of explanations on perceptions of voice assistants. *Proceedings of the ACM on Human-Computer Interaction*, *7*(CSCW1), 1–24.

Shlega, M., Maqsood, S., & Chiasson, S. (2022). Users, smart homes, and digital assistants: impact of technology experience and adoption. In *International conference on human-computer interaction* (pp. 422–443). Springer.

Shofolahan, T. O., & Kang, J. (2018). An integrated framework for modeling the influential factors affecting the use of voice-enabled IoT devices : A case study of amazon echo. *Asia Pacific Journal of Information Systems*, *28*(4), 320–349. http://dx.doi.org/10.14329/apjis.2018.28.4.320.

Shuhaiber, A., & Mashal, I. (2019). Understanding users' acceptance of smart homes. *Technology in Society*, *58*, Article 101110.

Skjuve, M., & Brandzaeg, P. B. (2019). Measuring user experience in chatbots: An approach to interpersonal communication competence. In *Internet science: INSCI 2018 international workshops, St. Petersburg, Russia, October 24–26, 2018, revised selected papers 5* (pp. 113–120). Springer.

Smith, Dinev, & Xu (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989. http://dx.doi.org/10.2307/41409970, arXiv:10.2307/41409970.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167–196. http://dx.doi.org/10.2307/249477.

Son, J.-Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, 503–529.

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*, Article 101199.

Song, M., Xing, X., Duan, Y., Cohen, J., & Mou, J. (2022). Will artificial intelligence replace human customer service? The impact of communication quality and privacy risks on adoption intention. *Journal of Retailing and Consumer Services*, *66*, Article 102900.

Suplet, M., Gómez Suárez, M., & Díaz-Martín, A. (2009). Customer perceptions of perceived risk in generic drugs: The Spanish market. *Innovar*, *19*, 53–64.

Tabassum, M., Kosiński, T., Frik, A., Malkin, N., Wijesekera, P., Egelman, S., et al. (2019). Investigating users' preferences and expectations for always-listening voice assistants. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *3*(4), 1–23. http://dx.doi.org/10.1145/3369807.

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, *29*(3), 821–826.

Tan, F. B., & Sutherland, P. (2005). Consumer trust: A multi-dimensional model. In *Advanced topics in electronic commerce, volume 1: vol. 1*, (p. 188). IGI Global.

Tastemirova, A., Schneider, J., Kruse, L. C., Heinzle, S., & Brocke, J. v. (2022). Microexpressions in digital humans: perceived affect, sincerity, and trustworthiness. *Electronic Markets*, *32*(3), 1603–1620.

Tenhundfeld, N. L., Barr, H. M., Emily, H., & Weger, K. (2021). Is my Siri the same as your Siri? An exploration of users' mental model of virtual personal assistants, implications for trust. *IEEE Transactions on Human-Machine Systems*, *52*(3), 512–521.

Tennant, R., Allana, S., Mercer, K., & Burns, C. M. (2022). Caregiver expectations of interfacing with voice assistants to support complex home care: Mixed methods study. *JMIR Human Factors*, *9*(2), Article e37688. http://dx.doi.org/10.2196/37688.

Tlili, A., Shehata, B., Adarkwah, M. A., Bozkurt, A., Hickey, D. T., Huang, R., et al. (2023). What if the devil is my guardian angel: ChatGPT as a case study of using chatbots in education. *Smart Learning Environments*, *10*(1), 15. http://dx.doi.org/10.1186/s40561-023-00237-x.

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

Trepte, S., Scharkow, M., & Dienlin, T. (2020). The privacy calculus contextualized: The influence of affordances. *Computers in Human Behavior*, *104*, Article 106115. http://dx.doi.org/10.1016/j.chb.2019.08.022.

Trivedi, J. (2019). Examining the customer experience of using banking chatbots and its impact on brand love: The moderating role of perceived risk. *Journal of Internet Commerce*, *18*(1), 91–111.

Tsu Wei, T., Marthandan, G., Yee-Loong Chong, A., Ooi, K.-B., & Arumugam, S. (2009). What drives Malaysian M-commerce adoption? An empirical analysis. *Industrial Management & Data Systems*, *109*(3), 370–388. http://dx.doi.org/10.1108/02635570910939399.

Uysal, E., Alavi, S., & Bezençon, V. (2022). Trojan horse or useful helper? A relationship perspective on artificial intelligence assistants with humanlike features. *Journal of the Academy of Marketing Science*, *50*(6), 1153–1175. http://dx.doi.org/10.1007/s11747-022-00856-9.

van Bussel, M. J. P., Odekerken-Schröder, G. J., Ou, C., Swart, R. R., & Jacobs, M. J. G. (2022). Analyzing the determinants to accept a virtual assistant and use cases among cancer patients: a mixed methods study. *BMC Health Services Research*, *22*, 890. http://dx.doi.org/10.1186/s12913-022-08189-7.

Van Der Goot, M. J., & Pilgrim, T. (2020). Exploring age differences in motivations for and acceptance of chatbot communication in a customer service context. In A. Følstad, T. Araujo, S. Papadopoulos, E. L.-C. Law, O.-C. Granmo, E. Luger, & P. B. Brandtzaeg (Eds.), *Chatbot research and design*: *vol. 11970*, (pp. 173–186). Cham: Springer International Publishing, http://dx.doi.org/10.1007/978-3-030-39540-7_12.

Van Deursen, A. J., Helsper, E. J., & Eynon, R. (2016). Development and validation of the internet skills scale (ISS). *Information, Communication & Society*, *19*(6), 804–823.

van Eeuwen, M. (2017). *Mobile conversational commerce: Messenger chatbots as the next interface between businesses and consumers* (Master's thesis), University of Twente.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, *46*(2), 186–204.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 157–178.

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*, Article 106763. http://dx.doi.org/10.1016/j.chb.2021.106763.

Vitak, J. (2015). Balancing privacy concerns and impression management strategies on facebook. In *Symposium on usable privacy and security* (pp. 22–24).

Vitak, J. (2016). A digital path to happiness?: Applying communication privacy management theory to mediated interactions. In *The routledge handbook of media use and well-being* (pp. 274–288). Routledge.

Vixen Labs (2023). AI consumer index. https://vixenlabs.co/research/ai-consumer-index-2023. (Accessed Online 13 December 2023).

Wald, R., Heijselaar, E., & Bosse, T. (2021). Make your own: The potential of chatbot customization for the development of user trust. In *Adjunct proceedings of the 29th ACM conference on user modeling, adaptation and personalization* (pp. 382–387).

Wang, W., & Benbasat, I. (2016). Empirical assessment of alternative designs for enhancing different types of trusting beliefs in online recommendation agents. *Journal of Management Information Systems*, *33*(3), 744–775.

Wang, Z., Mao, H., Li, Y. J., & Liu, F. (2017). Smile big or not? Effects of smile intensity on perceptions of warmth and competence. *Journal of Consumer Research*, *43*(5), 787–805.

Wang, Y.-Y., & Wang, Y.-S. (2022). Development and validation of an artificial intelligence anxiety scale: An initial application in predicting motivated learning behavior. *Interactive Learning Environments*, *30*(4), 619–634.

Waytz, A., Cacioppo, J., & Epley, N. (2010). Who sees human? The stability and importance of individual differences in anthropomorphism. *Perspectives on Psychological Science*, *5*(3), 219–232.

Weidmüller, L. (2022). Human, hybrid, or machine?: Exploring the trustworthiness of voice-based assistants. *Human-Machine Communication*, *4*, 85–110.

Weitz, K., Schiller, D., Schlagowski, R., Huber, T., & André, E. (2019). "Do you trust me?" Increasing user-trust by integrating virtual agents in explainable AI interaction design. In *Proceedings of the 19th ACM international conference on intelligent virtual agents* (pp. 7–9).

Xiao, S., & Benbasat, I. (2002). The impact of internalization and familiarity on trust and adoption of recommendation agents. Unpublished Working Paper.

Xu, K., Chan-Olmsted, S., & Liu, F. (2022). Smart speakers require smart management: two routes from user gratifications to privacy settings. *International Journal of Communication*, *16*, 23.

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

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 1.

Xu, H., & Gupta, S. (2009). The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. *Electronic Markets*, *19*, 137–149.

Xu, H., Gupta, S., Rosson, M., & Carroll, J. (2012). Measuring mobile users' concerns for information privacy. In *ICIS 2012 proceedings*.

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.

Yamagishi, T., & Yamagishi, M. (1994). Trust and commitment in the United States and Japan. *Motivation and Emotion*, *18*, 129–166.

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. http://dx.doi.org/10.1108/IMDS-01-2016-0017.

Yang, Y., Liu, Y., Li, H., & Yu, B. (2015). Understanding perceived risks in mobile payment acceptance. *Industrial Management & Data Systems*, *115*(2), 253–269.

Yao, Y., Basdeo, J. R., Mcdonough, O. R., & Wang, Y. (2019). Privacy perceptions and designs of bystanders in smart homes. *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW), 1–24. http://dx.doi.org/10.1145/3359161.

Ye, S., Ying, T., Zhou, L., & Wang, T. (2019). Enhancing customer trust in peer-to-peer accommodation: A "soft" strategy via social presence. *International Journal of Hospitality Management*, *79*, 1–10. http://dx.doi.org/10.1016/j.ijhm.2018.11.017.

Yoo, W.-S., Lee, Y., & Park, J. (2010). The role of interactivity in e-tailing: Creating value and increasing satisfaction. *Journal of Retailing and Consumer Services*, *17*(2), 89–96.

Zeissig, E.-M., Lidynia, C., Vervier, L., Gadeib, A., & Ziefle, M. (2017). Online privacy perceptions of older adults. In *Human aspects of IT for the aged population. applications, services and contexts: third international conference, ITAP 2017, held as part of HCI international 2017, Vancouver, BC, Canada, July 9-14, 2017, proceedings, part II 3* (pp. 181–200). Springer.

Zeng, E., Mare, S., & Roesner, F. (2017). End user security and privacy concerns with smart homes. In *Thirteenth symposium on usable privacy and security* (pp. 65–80).

Zhang, S., Meng, Z., Chen, B., Yang, X., & Zhao, X. (2021). Motivation, social emotion, and the acceptance of artificial intelligence virtual assistants—Trust-based mediating effects. *Frontiers in Psychology*, *12*, Article 728495.

Zhou, T. (2011). The impact of privacy concern on user adoption of location-based services. *Industrial Management & Data Systems*, *111*(2), 212–226. http://dx.doi.org/10.1108/02635571111115146.

Zlatolas, L. N., Welzer, T., Hölbl, M., Hericko, M., & Kamisalic, A. (2019). A model of perception of privacy, trust, and self-disclosure on online social networks. *Entropy*, *21*, URL: https://api.semanticscholar.org/CorpusID:201264486.

Zwakman, D. S., Pal, D., & Arpnikanondt, C. (2021). Usability evaluation of artificial intelligence-based voice assistants: The case of amazon Alexa. *SN Computer Science*, *2*(1), 28. http://dx.doi.org/10.1007/s42979-020-00424-4.