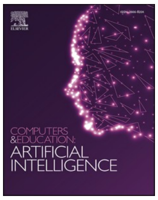
Contents lists available at ScienceDirect

Computers and Education: Artificial Intelligence

journal homepage: www.sciencedirect.com/journal/computers-and-education-artificial-intelligence



Safer interaction with IVAs: The impact of privacy literacy training on competent use of intelligent voice assistants

André Markus[a,*], Maximilian Baumann[b], Jan Pfister[c], Astrid Carolus[b], Andreas Hotho[c], Carolin Wienrich[a]

[a] Psychology of Intelligent Interactive Systems, Institute Human-Computer-Media, Julius-Maximilians-University Wuerzburg, Emil-Fischer-Straße 50, 97074, Wuerzburg, Germany
[b] Media Psychology, Institute Human-Computer-Media, Julius-Maximilians-University Wuerzburg, Oswald-Külpe-Weg 82, 97074, Wuerzburg, Germany
[c] Chair of Data Science (Informatic X), Julius-Maximilians-University Wuerzburg, Emil-Fischer-Straße 50, 97074, Wuerzburg, Germany

ARTICLE INFO

Additional Keywords and Phrases:
Intelligent voice Assistant
Privacy literacy
Smart speaker
Data protection
Digital interaction literacy
Human-Computer interaction

ABSTRACT

Intelligent voice assistants (IVAs) are widely used in households but can compromise privacy by inadvertently recording or encouraging personal disclosures through social cues. Against this backdrop, interventions that promote privacy literacy, sensitize users to privacy risks, and empower them to self-determine IVA interactions are becoming increasingly important. This work aims to develop and evaluate two online training modules that promote privacy literacy in the context of IVAs by providing knowledge about the institutional practices of IVA providers and clarifying users' privacy rights when using IVAs. Results show that the training modules have distinct strengths. For example, Training Module 1 increases subjective privacy literacy, raises specific concerns about IVA companies, and fosters the intention to engage more reflectively with IVAs. In contrast, Training Module 2 increases users' perceptions of control over their privacy and raises concerns about devices. Both modules share common outcomes, including increased privacy awareness, decreased trust, and social anthropomorphic perceptions of IVAs. Overall, these modules represent a significant advance in promoting the competent use of speech-based technology and provide valuable insights for future research and education on privacy in AI applications.

1. Introduction

The proliferation of intelligent voice assistants (IVAs) is increasing. They are integrated into mobile and stationary devices such as smartphones, smartwatches, tablets, cars, and smart speakers (Fowler, 2018). One of the key advantages of IVAs in daily use, such as Alexa or Google Assistant, is their conversational interface. Since the interaction is through natural language, it is more intuitive and easier to use than web and mobile interfaces based on manual keyboard input (Zhong & Yang, 2018). Advanced AI technologies are employed by IVAs to process complex data in real time, enabling the automation of tasks such as appointment reminders, music playback, and the delivery of information on demand. However, IVAs raise privacy and security concerns (Agrawal, Gans, & Goldfarb, 2018; Shin, Zhong, & Biocca, 2020) because they collect sensitive and private data such as users' voice requests, location history, contacts, calendars, browsing history, and purchase history (Gardiner, 2018). A report found that 41% of participants expressed concerns and distrust towards IVAs, with many believing that these devices invade privacy through passive eavesdropping (Olson & Kemery, 2019). Approximately 52% of respondents also indicated that they were concerned about the security of their personal data. In particular, the constant activity of microphones and connection to the Internet is associated with concerns (Easwara Moorthy & Vu, 2014). The perceived risks in this area lead people to refrain from using IVAs or some of their features or stop using them altogether (O`Brien & Sohail, 2020). On the other hand, some users are relatively unconcerned about the privacy risks posed by IVAs. This is because, for example, they are not sufficiently informed about the risks associated with IVAs and potential effective privacy safeguards, and they set aside privacy concerns in favor of convenience (Kang, Dabbish, Fruchter, & Kiesler, 2015; Lau, Zimmerman, & Schaub, 2018; Tabassum, Kosinski, & Lipford, 2019). This demonstrates the need for measures that enable people to realistically assess the privacy risks posed by IVAs and empower them to protect themselves. Although there are a few

* Corresponding author.
E-mail address: andre.markus@uni-wuerzburg.de (A. Markus).

https://doi.org/10.1016/j.caeai.2025.100372
Received 9 October 2024; Received in revised form 24 December 2024; Accepted 19 January 2025
Available online 21 January 2025

empirically validated training programs to promote digital privacy literacy (e.g., Desimpelaere, Hudders, & Van de Sompel, 2020; Sideri, Kitsiou, Tzortzaki, Kalloniatis, & Gritzalis, 2019), our review highlights a significant gap in privacy literacy training focused on IVAs, particularly those that follow a specific curricular framework to develop the skills necessary for competent IVA interaction. Such training is crucial for ensuring safe, empowered, and competent interactions with IVAs (Carolus, Augustin, Markus, & Wienrich, 2023). Therefore, this work addresses the research questions and gaps on 1) how effective training in this area should be designed and 2) what impact this training has on parameters of competent IVA interaction.

2. Background and literature review

2.1. IVAs as privacy Infiltrators

User privacy concerns about IVAs include authentication, always-on mode, replay attacks, and reliance on cloud infrastructure (Sharif & Tenbergen, 2020). For example, IVAs can be activated by others nearby within the user's hearing and speaking range, exposing sensitive personal data such as calendar information or messages, which are not safeguarded by passwords or fingerprints (Courtney, 2017; Pal, Arpnikanondt, Razzaque, & Funilkul, 2020). Another issue is that IVAs are always listening: Even a single wake-word utterance or similar phrases immediately record potentially sensitive conversations, which are then sent to the provider's cloud (Edu, Such, & Suarez-Tangil, 2020). Many users are unaware of the extent of this data collection and how their data is used or shared (e.g., for advertising purposes), leading to a sense of losing privacy control (Abdi, Zhan, Ramokapane, & Such, 2021; Bonilla & Martin-Hammond, 2020; Choi, Park, & Jung, 2018; Malkin et al., 2019; Son & Kim, 2008; Tabassum et al., 2019). Users frequently perceive themselves as powerless in the face of privacy breaches due to a lack of privacy-related knowledge (Emami-Naeini, Dixon, Agarwal, & Cranor, 2019; Huang, Han, & Zhu, 2021; Jacobsson & Davidsson, 2015; Lau et al., 2018). This results in dichotomous perceptions among users, with some users underestimating or overestimating the privacy risks. Overestimating privacy risks is leading users to limit or abandon the use of IVAs (Cobb et al., 2021, pp. 54–75; Easwara Moorthy & Vu, 2014; Pradhan, Mehta, & Findlater, 2018; Tabassum et al., 2019). If privacy risks are underestimated, users are more likely to disregard privacy concerns and disclose more personal data to take advantage of the perceived benefits of IVAs (Kang & Oh, 2023; Ketelaar & Van Balen, 2018). Wienrich, Reitelbach, and Carolus (2021) discovered that users are likelier to share sensitive information with IVAs if presented as health experts. This suggests that users may be motivated to disclose personal information by a) a desire to appear as informed as possible and b) a lack of awareness of the risks of disclosing personal information. However, users often believe their personal data would be irrelevant to providers (Lau et al., 2018), which shows that many users do not clearly understand the value of their IVA data to the underlying IVA providers (cf. Jayatilleke, Thelijjagoda, & Pathirana, 2019) and highlights the need for privacy literacy training to make users aware of the importance of the data.

2.2. Relevance of privacy literacy training

Various studies have identified a lack of understanding and misconceptions about the privacy risks associated with the use of IVAs (Cobb et al., 2021, pp. 54–75; Lau et al., 2018). However, there is a lack of empirical research on promoting privacy literacy in the context of IVAs. Privacy literacy is essential for enabling individuals to interact with IVAs self-determined and securely (Carolus, Augustin, et al., 2023). In order to reinforce this, it is essential to disseminate knowledge regarding institutional practices in the exploitation of personal data by providers so that users are aware of their privacy rights (Carolus, Augustin, et al., 2023). To adopt data privacy-friendly behavior, being aware of your privacy and the associated risks is important. For instance, internet users are more likely to make informed decisions about their privacy the more they understand data processing (Baruh, Secinti, & Cemalcilar, 2017; Boerman, Kruikemeier, & Zuiderveen Borgesius, 2021; Büchi, Just, & Latzer, 2017; Chetty et al., 2018). Moreover, individuals with greater privacy literacy in social networks are more inclined to frequently update their privacy settings and show reduced engagement in risky online behaviors due to heightened awareness of privacy risks (Bartsch & Dienlin, 2016; Vanderhoven, Schellens, & Valcke, 2016). A more profound comprehension of the potential privacy risks positively influences the perception of one's capacity to safeguard information, which motivates users to implement protective measures (Arachchilage & Love, 2014). These studies indicate that interventions positively affect individuals' privacy-friendly experiences and behavior. For this reason, this study has developed two training modules designed to promote privacy literacy in the context of IVAs. The efficacy of the modules is also evaluated concerning several variables.

2.2.1. Privacy literacy and privacy aspects

Privacy literacy refers to awareness and knowledge about institutional data practices (e.g., providers' use of usage data), privacy risks, and privacy protection strategies (Bartsch & Dienlin, 2016; Carolus, Augustin, et al., 2023). Studies show that people who are informed about the institutional data practices of providers have greater **privacy concerns** about them and exhibit more privacy-protective behavior, such as providing an incomplete name or being less willing to **disclose personal information** (Kim, Chung, & Ahn, 2014; Park, 2013; Youn, 2009). **Trust** is crucial in sharing personal information, as recognizing privacy risks can erode trust and decrease the willingness to disclose, thereby protecting privacy (Gupta, Hooda, Jeyaraj, Seddon, & Dwivedi, 2024; Hallam & Zanella, 2017; Liao, Liu, & Chen, 2011; Mesch, 2012). The greater the level of privacy literacy, the more carefully users select the topics of conversation to be discussed around the IVA, and the lower the level of trust in IVAs (Dienlin & Metzger, 2016; Harborth & Pape, 2020; Liao, Vitak, Kumar, Zimmer, & Kritikos, 2019). Furthermore, **privacy awareness** can be defined as a person's knowledge and understanding of data use, privacy risks, and privacy protection actions (Xu, Dinev, Smith, & Hart, 2008). In light of this definition, the present work postulates a positive effect on privacy awareness of training that promotes privacy-related understanding and knowledge of IVAs. In order to protect against potential privacy threats and to feel comfortable sharing personal information, perceived **privacy control** is of great importance (Bartsch & Dienlin, 2016). Studies show that a better understanding of privacy risks increases perceived privacy control (Arachchilage & Love, 2014; Bandyopadhyay, 2012; Büchi et al., 2017). Other research also indicates that knowledge of how companies process data, who is responsible for data protection, and what rights users have when they process their data increases the perceived privacy control (Prince, Omrani, & Schiavone, 2024). Under the representative null hypothesis that privacy literacy training does not affect the variables studied, the following alternative hypotheses regarding IVAs are formulated.

H1. Conducting privacy literacy training positively affects subjective privacy literacy.

H2. Conducting privacy literacy training has a positive effect on privacy concerns.

H3. Conducting privacy literacy training has a negative effect on a) trust and b) self-disclosure towards IVAs.

H4. Conducting privacy literacy training positively affects a) privacy awareness and b) privacy control.

2.2.2. Privacy literacy and usage aspects

Privacy literacy impacts user acceptance variables such as ease of use, enjoyment, and intention to use. Privacy settings in technological devices are often not implemented by users because they are perceived as too complex, and when technical aspects are perceived as complex, **ease of use** decreases (Hasan, 2007; Rudolph, Feth, & Polst, 2018). In terms of **enjoyment**, learning about privacy risks in technologies has been found to result in a reduction in enjoyment (Hwang & Kim, 2007; Miltgen, Popovič, & Oliveira, 2013). Research demonstrated that education about privacy risks in an educational intervention increased privacy concerns (Sideri et al., 2019). Privacy concerns, in turn, can reduce **intentions to use** an application, such as online booking websites (Yi, Yuan, & Yoo, 2020). Additionally, a study on smartphone usage revealed that as privacy concerns intensified, the likelihood of utilizing the device diminished (Xu, Gupta, Rosson, & Carroll, 2012). Based on this evidence, it can be assumed that.

H5. Conducting privacy literacy training has a negative effect on a) ease of use, b) enjoyment, and c) intention to use.

2.2.3. Privacy literacy and social perception

Users perceive IVAs as social due to anthropomorphic features, e.g., dialog ability and human-like names (Voorveld & Araujo, 2020). This social perception can reduce perceived risks and privacy concerns and increase negative privacy consequences such as over-trust and higher unconscious self-disclosure (Couper, Tourangeau, & Steiger, 2001; de Kloet & Yang, 2022; Ischen, Araujo, Voorveld, van Noort, & Smit, 2020; Monteleone, van Bavel, Rodríguez-Priego, & Esposito, 2015; Nass & Brave, 2005; Sciuto, Saini, Forlizzi, & Hong, 2018; Wienrich et al., 2021). Training should, therefore, aim to reduce anthropomorphic perceptions that counteract these dangers (Carolus, Augustin, et al., 2023). Markus, Pfister, Carolus, Hotho, and Wienrich (2024b) showed that promoting knowledge of how IVAs work and processing their usage data breaks down social perceptions of IVAs. Similarly, this study hypothesizes that knowing how IVAs can intrude on users' privacy could reduce anthropomorphic perceptions. Therefore, it is hypothesized.

H6. Conducting privacy literacy training has a negative effect on social-anthropomorphic perceptions of IVAs.

2.2.4. Privacy literacy and self-determined interactions

In addition to privacy literacy, reflection, and emotion regulation skills are important for self-determined interaction with IVAs (Carolus, Augustin, et al., 2023). **Reflection** entails questioning one's usage behavior concerning individual needs, ethical aspects, and possible risks and is influenced by existing knowledge concepts (Carolus, Augustin, et al., 2023; Hatlevik, 2012; Kember, 2008). Given that a comprehensive knowledge base is a fundamental prerequisite for the effective implementation of reflection (Schön, 2017), providing knowledge on privacy-related topics could serve as a robust foundation for the advancement of reflection. Emotion-regulating processes such as **indulgence** can enhance the quality of interaction with IVAs and increase behavioral control in AI interactions, for instance, when voice commands are misunderstood (Carolus, Koch, Straka, Latoschik, & Wienrich, 2023; Schweitzer, Belk, Jordan, & Ortner, 2019). While indulgence is beneficial in IVA interactions, it is possible that a negative effect of privacy literacy training can be assumed. Recognizing privacy risks can give rise to negative emotions such as frustration, fear, or regret, which may result in users becoming less indulgent in their interactions with IVAs (Cho, Li, & Goh, 2020; McCullough, 2000). Based on the literature, it can be assumed that.

H7. Conducting privacy literacy training has a) a positive effect on reflection and b) a negative effect on indulgence.

2.3. Current study

The existing literature indicates that privacy literacy can positively contribute to the competent handling of IVAs and can support the assessment of possible risks and the reduction of misunderstandings (Carolus, Augustin, et al., 2023). In addition, recent studies show that online training can enhance skills in the competent and self-determined use of IVAs, such as AI understanding (Markus, Pfister, Carolus, Hotho, & Wienrich, 2024a). In this work, we leverage this potential to develop and evaluate training that specifically promotes privacy literacy in the context of IVAs. In **two studies**, one training module each will be developed and examined concerning its effect on privacy literacy, privacy-related experiences, usage aspects, social perceptions, and aspects of self-determined interaction, using an experimental pre-post design. The conceptual basis for the training is the Digital Interaction Literacy (DIL) model (Carolus, Augustin, et al., 2023), which offers a holistic approach to promoting privacy literacy in the context of IVAs. **Training Module 1** focuses on institutional data practices and provides insight into what IVA providers know about users and the extent of usage data they can access. **Training Module 2** addresses relevant privacy regulations, security issues related to IVAs, and user privacy rights. Both modules follow the same training design and evaluation methodology to assess the parameters of competent IVA interaction, ensuring a coherent investigation. Combining the two studies in one work provides a comprehensive assessment of privacy literacy and competent IVA interaction, covering institutional data practices (Study 1) and legal/privacy aspects (Study 2). This enables a thorough assessment of the effectiveness of the training modules in promoting self-determined interaction and privacy protection, contributing to a more accurate assessment of potential risks and a reduction of misunderstandings about IVAs and AI applications in general.

3. Methods

3.1. General design principles and structure of training modules

The content of the training modules on privacy literacy is based on the DIL model (Carolus, Augustin, et al., 2023). Specific content and instructional texts were developed based on literature research, e.g., the European Data Protection Board (2021) and the General Data Protection Regulation (GDPR). Training Module 1 "Institutional Practices" explains the business models of IVA providers and what they know about users based on their stored voice data. Training Module 2 "User Rights and Security Gaps" explains users' rights when using IVAs, where security gaps occur, and related data protection regulations abroad. Further details on the content of the training modules can be found in the corresponding sections of Study 1 and 2.

The training modules were developed using the principles of multimedia learning media design, which aims to optimize learning experiences (Clark & Mayer, 2016; Mayer, 2014). Instructional psychology design recommendations that promote learning were applied, e.g., the variability effect (Sweller, van Merriënboer, & Paas, 2019), the signaling effect (Mayer & Fiorella, 2014), and the Hamburg comprehensibility concept (Langer, von Thun, & Tausch, 2019). Within the training modules, back and forward navigation buttons allowed participants to revisit content as needed, facilitating learner-driven exploration of the material that promotes effective learning (Mayer, 2014; Spanjers, Van Gog, & van Merriënboer, 2010). Additionally, decorative images with learning-relevant and positive valence were integrated into the instructional texts to improve the learning experience (Schneider, Nebel, & Rey, 2016). Technically, the training modules were implemented using the e-learning tool Captivate Classic (Adobe Captivate, 2019) and structured as follows: 1) A welcoming screen, 2) Learning objectives were presented, 3) Instructional texts were presented, and 4) Exercises on the learning content were provided (e.g., multiple choice, gap texts, drag-and-drop), some of which were based on and inspired by previous studies measuring privacy literacy and knowledge (e.g., Park, 2013; Trepte et al., 2015). The exercises should engage participants actively in the learning content (Wilder, Flood, & Stromsnes, 2001; Zarei, 2013). If a task was answered incorrectly, it could be repeated two times. Participants were then presented with a sample solution, regardless of whether they had solved the task correctly or not. This ensured that all participants had access to the same level of information. Fig. 1 shows excerpts from Training Module 1, while Table A1 presents examples of exercises.

3.2. Measurements

The measurement instruments used in the two studies are presented below and briefly summarized in Table A2. All measurement instruments contained items rated on a 5-point Likert scale (1 = not at all; 5 = totally).

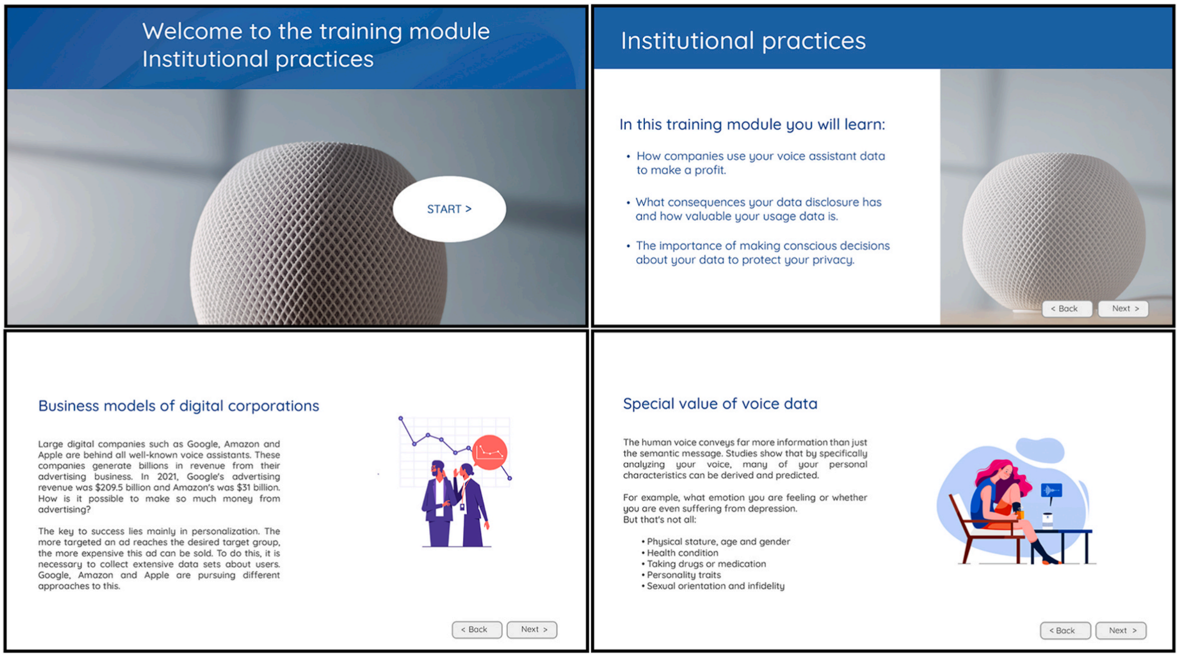
Privacy Aspects. Participants' subjective privacy literacy was assessed using the *Subjective Privacy Literacy Scale* (SPL; $\alpha = .83$) by Ma and Chen (2023) and adapted IVAs. The three-item scale captures knowledge and understanding of how organizations manage and process personal information (e.g., "Overall, I have a very good understanding of how organizations collect and manage my personal information."). To gain more insight into participants' privacy concerns regarding IVA use, the subscales *device privacy concerns* (5 items, e.g., "The voice assistant turning itself on when it should not.", $\alpha = .89$), *stranger privacy concerns* (4 items, e.g., "Strangers listening to my conversations with the voice assistant.", $\alpha = .95$) and *company privacy concerns* (8 Items, e.g., "Amazon/Google/Apple insufficiently protecting my Alexa data.", $\alpha = .94$) were used (Lutz & Newlands, 2021). *Trust* in IVAs was measured with two items from Wienrich et al. (2021) (e.g., "I think voice assistants are trustworthy.", $\alpha = 70$). The *Personal Information Disclosure* subscale by Pal, Arpnikanondt, and Razzaque (2020) was used to measure the effect of training on willingness to share personal information with IVAs (*self-disclosure*) (3 items, e.g., "I am likely to disclose my personal information.", $\alpha = .94$). *Privacy awareness* ($\alpha = .87$) in the IVA context was measured with three items from Dinev and Hart (2005) (e.g., "I am aware of privacy issues and practices in our society."). *Perceived privacy control* ($\alpha = .89$) was measured with four items from Xu et al. (2012) and adapted to IVAs (e.g., "I believe I have control over how personal information is used by the voice assistant.").

User Acceptance. To determine the effect of training modules on aspects of IVA acceptance, the three IVAs adapted subscales *ease of use* (3 items, e.g., "I find voice assistants easy to use.", $\alpha = .73$), *enjoyment* (5 items, e.g., "I find voice assistants enjoyable.", $\alpha = .77$), *intention to use* (3 items, e.g., "I plan to use voice assistants in the future.", $\alpha = .94$) from Heerink, Krose, Evers, and Wielinga (2009) were used.

Anthropomorphization. To assess the impact of the training modules on the anthropomorphic perception of IVAs, the *Sociability* subscale (4 items, $\alpha = .93$) of the Human-Robot Interaction Evaluation Scale (HRIES) from Spatola, Kühnlenz, and Cheng (2021) was employed. Participants indicated how much they associated specific terms (e.g., warm, likable) with IVAs.

Reflection and Indulgence. In this study, the *Reflection* (8 items, e.g., "I reflect on my interaction with voice assistants.", $\alpha = .91$) and *Indulgence* (3 items, e.g., "I am indulgent when voice assistants make mistakes.", $\alpha = .87$) scales by Markus et al. (2024b) were used. The Reflection subscale assesses the intention to reflect on one's own IVA usage, usage consequences, and expectations of the systems. The Indulgence subscale describes the intention to indulge in negative experiences with IVAs.

Training Quality. The evaluation of training quality is crucial for the efficiency, validity, and optimization of training as well as for the successful transfer of learned behaviors (Goldstein & Ford, 2002; Ritzmann, Hagemann, & Kluge, 2014). Predictors such as perceived usefulness and difficulty of training are critical for effective learning, transfer of learning into practice, and demonstration of skills (Alliger, Tannenbaum, Bennett Jr, Traver, & Shotland, 1997; Gegenfurtner, 2011; Warr & Bunce, 1995; Warr, Allan, & Birdi, 1999). In order to ensure a high level of training quality, the *Training Evaluation Inventory* (Ritzmann, Hagemann, & Kluge, 2020) was used to measure key predictors of training quality. The inventory includes the subscales *Subjective Fun* (3 items, e.g., "The learning was fun.", $\alpha = .81$), *Perceived Usefulness* (4 items, e.g., "I derive personal use from this training.", $\alpha = 89$), *Perceived Difficulty* (4 items, e.g., "The contents were comprehensible.", $\alpha = .73$), *Subjective Knowledge Growth* (3 items, e.g., "I will be able to remember the new themes well.", $\alpha = .75$), and *Attitude toward Training* (3 items, e.g., "I would recommend this training to my colleagues.", $\alpha = .81$). The results indicate the quality of the learning experience, the validity of the training modules and provide insight into potential training improvements.


Welcome to the training module
Institutional practices

Institutional practices

In this training module you will learn:

- How companies use your voice assistant data to make a profit.
- What consequences your data disclosure has and how valuable your usage data is.
- The importance of making conscious decisions about your data to protect your privacy.

Business models of digital corporations

Large digital companies such as Google, Amazon and Apple are behind all well-known voice assistants. These companies generate billions in revenue from their advertising business. In 2021, Google's advertising revenue was $209.5 billion and Amazon's was $31 billion. How is it possible to make so much money from advertising?

The key to success lies mainly in personalization. The more targeted an ad reaches the desired target group, the more expensive this ad can be sold. To do this, it is necessary to collect extensive data sets about users. Google, Amazon and Apple are pursuing different approaches to this.

Special value of voice data

The human voice conveys far more information than just the semantic message. Studies show that by specifically analyzing your voice, many of your personal characteristics can be derived and predicted.

For example, what emotion you are feeling or whether you are even suffering from depression.
But that's not all:

- Physical stature, age and gender
- Health condition
- Taking drugs or medication
- Personality traits
- Sexual orientation and infidelity

Fig. 1. Exemplary excerpts from Training Module 1.

3.3. Procedure

Fig. 2 shows the schematic sequence of the two studies. Each training module took approximately 25 min to complete, including exercises. The two training modules were conducted as an online study using the *SoSci Survey* web application (Leiner, 2024), which also included a randomizer to assign participants randomly to one of the training modules. After the participants gave their consent for data collection and agreed to the privacy policy, an introduction was given in which IVAs were defined as voice-based AI systems that are integrated into many everyday applications (e.g., smartphones, smart speakers, and navigation devices). The questionnaires described in Section 3.2 were then completed (pretest). The participants then started the training, which included learning the content and performing the exercises. The online training modules were completed independently, with participants free to choose their own time and place. They were instructed to work in a quiet environment with a stable internet connection and to complete the training without interruptions. There was no time limit for completing the training modules, which supported autonomous and individualized learning, promoting effective learning (Mayer, 2014; Rey et al., 2019; Spanjers et al., 2010). Immediately after the training, the post-test began, and the participants were given the same questionnaires as the pretest. The training quality was also evaluated. Finally, the participants' demographic data (age, gender) were recorded, and the purpose of the study was explained.

3.4. Data analysis

This paper presents hypotheses tests conducted assuming that the training modules influence the variables investigated in the study. Conformation of the hypotheses would entail rejecting the superior null hypothesis that the training modules do not influence these variables. Student's *t*-tests for dependent samples were used to analyze changes in the dependent variables between the pretest and the post-test. The significance level was set at $\alpha < .05$. To identify subtle changes and trends, marginal significant effects ($p < .10$) were also considered. Given the exploratory approach of the training study, the Benjamini-Hochberg correction is used to minimize the risk of alpha error (false positives) while still identifying relevant effects without reducing statistical power through excessive conversation correction (Benjamini & Hochberg, 1995; Storey, 2002). To determine the sample size, we calculated the required sample size using *G*Power* software (Faul, Erdfelder, & Buchner, 2007), referring to comparable studies on the effects of privacy literacy training, such as Desimpelaere et al. (2020), which reported an effect size of $d = 0.81$. With this effect size and a power of 0.95, 18 participants would be needed to detect a significant result with a one-tailed paired *t*-test ($\alpha = .05$). To further strengthen the robustness and statistical validity of the results, we followed the established guideline of a minimum sample size of $N = 30$, which is considered adequate to satisfy the assumptions of the central limit theorem and ensure the normality of the sampling distribution of the mean (Aron, Aron, & Coups, 2014; Cheung & Slavin, 2013; Memon et al., 2020; Pagano, 1990). Specifically for *t*-tests, the analyses by Sawilowsky and Blair (1992) confirm the robustness of t-tests with sample sizes ranging from $N = 25$–30. To ensure data quality, four control questions were developed for each study (e.g., "Mark the middle of the scale"). Participants who answered two or more of the control questions incorrectly were excluded from the data analysis to ensure the results' quality and reduce bias due to unconscious errors (e.g., due to lack of attention) or hasty responses (Meade & Craig, 2012; Thielsch & Hirschfeld, 2021). No predefined quality criteria or benchmarks for "good training" exist in the Training Evaluation Inventory (Ritzmann et al., 2020). Therefore, this study defined ratings of 3.0 and above as satisfactory, representing above-average performance on a 5-point Likert scale.

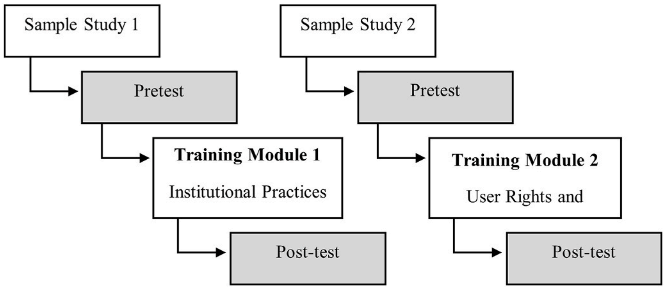


Fig. 2. Illustration of the experimental procedure.

4. Study 1: Institutional practices

4.1. Content of Training Module 1

Training Module 1 "Institutional Practices"[1] provides an understanding of how IVAs can interfere with privacy and insight into users' personal data, which is important for comprehensive privacy literacy (Carolus, Augustin, et al., 2023; Trepte et al., 2015). The training is divided into three chapters: **Chapter 1** examines the business models of prominent IVA providers (such as Amazon and Google) and elucidates the personal data they monitor from users and the strategic utilization of IVA data by providers to generate profit. It shows how companies collect vast amounts of user data, such as browsing habits, location, Wi-Fi connections, and personal details like age, gender, and contacts, to create detailed advertising profiles for targeted marketing. For example, it is explained that Amazon primarily uses shopping behavior and media consumption data, while Google uses data from Android devices, search activities, and location tracking to place personalized advertising. **Chapter 2** elucidates the consequences for users if they disclose data to the provider. It highlights the potential for classifying user similarities based on large amounts of user data, which could facilitate personalized and targeted advertising. So, for example, price changes in online stores can be influenced by personalized profiles: users deemed less price-sensitive may be shown higher prices, while certain offers or discount codes are strategically placed at the right time based on predictions of user behavior. Furthermore, the chapter explains the risks posed by hacker attacks, which can result in the theft of user profiles or their illegal resale. **Chapter 3** deals with the special and unique value of the human voice and the knowledge that can be derived from it (González-Rodríguez, Toledano, & Ortega-García, 2008). It describes the predictions and insights that can be derived by analyzing the user's voice, such as emotions, age, gender, sleep problems, drug use, personality traits, and sexual orientation (Guidi, Gentili, Scilingo, & Vanello, 2019; Suffoletto, Anwar, Glaister, & Sejdic, 2023; Sulpizio et al., 2015; Thoret, Andrillon, Gauriau, Leger, & Pressnitzer, 2024; Zaman, Sadekeen, Alfaz, & Shahriyar, 2021). The chapter emphasizes that the voice conveys much more than just the words spoken, offering a window into emotional states, health concerns, and psychological characteristics. The training module includes exercises in a multiple-choice format. These tasks require the learner to apply the previously learned material through recognition and transfer tasks. Examples of these tasks are presented in Table A1.

4.2. Participants

The sample consisted of $N = 36$ participants ($n_{\text{male}} = 16$, $n_{\text{female}} = 18$, $n_{\text{diverse}} = 2$) recruited from the Prolific panel (https://www.prolific.com/). During recruitment, filters were applied to select relevant participants from the Prolific panel. Participants were required to indicate

[1] Training Module 1: https://motiv.professor-x.de/train/PV1_v6.0JS.zip/index.html.

fluency in German in response to the question, "Which of the following languages are you fluent in?" to ensure comprehension of the study content. A further filter ensured that participants owned and used an intelligent voice assistant, requiring them to select IVAs from a list of internet-enabled products they already owned to qualify for the study. The mean age was 34.61 years (*SD* = 12.52; range = 19–73) (cf. Table A3). The majority of participants reported using IVAs daily (never = 3%; less than monthly = 3%; monthly = 8%; 2–3 times per month = 14%; weekly = 14%; 2–3 times per week = 22%; daily = 36%). Participants received monetary compensation (£8.92/hr).

4.3. Measures

The measuring instruments described in Section 3.2 were used to evaluate the effectiveness of the training module.

4.4. Results

The results of the analysis are presented in Table 1. Regarding privacy aspects, *subjective privacy literacy* has increased significantly, as predicted. Also, *privacy concerns* about devices and strangers were marginally significantly higher after training, while concerns about the company increased significantly. Similarly, as hypothesized, *trust* and *self-disclosure* were significantly reduced after the training. In line with the hypothesis, *privacy awareness* increased significantly after the training, while contrary to expectations, the training did not affect *privacy control*. Regarding the usage aspects, the expected effect of the training was confirmed by a negative change in *enjoyment* and *intention to use* the IVAs. As predicted, the training effect on *ease of use* was marginally significant and negative. Furthermore, a reduction in *social-anthropomorphic perception* was found as an aspect of social perception, which was in line with the hypothesis. In the context of self-determined interaction, there was a significant increase in *reflection* and a significant decrease in *indulgence* after the training. In terms of *training quality*, all criteria met a satisfactory level: Subjective Fun (*M* = 4.14, *SD* = 0.67), Perceived Usefulness (*M* = 4.22, *SD* = 0.54), Perceived Difficulty (*M* = 4.13, *SD* = 0.58), Subjective Knowledge Growth (*M* = 4.13, *SD* = 0.60) and Attitude towards Training (*M* = 4.18, *SD* = 0.52).

4.5. Discussion

Training Module 1 provides information about IVA providers' business practices, their knowledge about users, and the value of users' voice data, central to strong privacy literacy (Carolus, Augustin, et al., 2023). Results showed that the training improved participants' subjective privacy literacy (H1 confirmed). In addition, the training significantly increased concerns about IVA companies and tended to raise concerns about devices and strangers as well (H2 confirmed). The training may have triggered a surprising realization that providers collect potentially more personal data than expected (e.g., GPS data, IP address, psychological aspects), leading to increased privacy concerns. In addition, privacy concerns may have increased as respondents have become more aware that, despite the data security precautions taken by IVA providers, the security of personal data cannot be fully guaranteed (e.g., by hackers) (Cespedes & Smith, 1993; Wang, Sun, Dai, Zhang, & Hu, 2019). These results support other research, which found that negative attitudes toward data processors correlate with higher privacy literacy (Desimpelaere et al., 2020).

The training resulted in more privacy-friendly experiences and behavioral intentions: Trust in IVAs and willingness to disclose personal information to them decreased (H3a-b confirmed). Consistent with other research, lower levels of trust may be associated with greater privacy sensitivity (Harborth & Pape, 2020), while lower levels of willingness to self-disclose may indicate greater awareness of privacy risks (Dinev & Hart, 2006). The observed change in willingness to disclose personal information can be attributed to the perception that privacy is not adequately protected, as evidenced by other studies (Gilbert, 2001; Hinde, 1998). The training increased privacy awareness (H4a confirmed) but not privacy control (H4b not confirmed). This effect on privacy awareness is consistent with studies showing that a better understanding of how providers use data and the risks involved increases privacy awareness (Xu et al., 2008). The lack of effect on privacy control is not unexpected, given that the training also highlights the risks of losing control, increasing privacy concerns (Dinev & Hart, 2006).

Training decreased the user acceptance variables of ease of use, enjoyment (marginally significant), and intention to use in the context of IVAs (H5a-c confirmed). This may be due to increased concerns about data security, which other studies have shown negatively impact user acceptance and intention to use (Angst & Agarwal, 2009; Eastlick, Lotz, & Warrington, 2006; Hasan, 2007; Maier, Laumer, Weinert, & Weitzel, 2015; Miltgen et al., 2013; Yi et al., 2020). Furthermore, training reduced social anthropomorphic perceptions of IVAs (H6 confirmed). This is consistent with Markus et al. (2024b), who showed that knowledge of data processing by IVAs reduces their social perceptions. Interestingly, privacy concerns are reduced when users perceive IVAs as human (de Kloet & Yang, 2022). However, the training increased concerns regarding the privacy of the IVAs, which are typically perceived anthropomorphically. This could indicate that the training has a compensatory effect, whereby anthropomorphic perception is reduced through risk sensitization. Training increased intentions to use IVAs reflectively and decreased indulgence toward IVAs (H7a-b confirmed). This is consistent with previous studies showing that training can expand privacy-relevant knowledge concepts, thereby improving the conditions for reflection (Hatlevik, 2012; Kember, 2008). The negative effect on indulgence could be interpreted as a reaction to the negative emotions (cf. Cho et al., 2020; McCullough, 2000) caused by the training. For example, the acquired knowledge and awareness of the profit motives of IVA providers, the risks to one's privacy, or the large amount of data collected may have triggered unpleasant feelings such as fear or worry.

5. Study 2: User rights and security gaps

5.1. Content of Training Module 2

Training Module 2 "User Rights and Security Gaps"[2] explains users' rights when interacting with IVAs. In addition, security gaps are addressed, and the data protection regulations applicable abroad are explained. This learning content is considered important for strong privacy literacy (Carolus, Augustin, et al., 2023; Trepte et al., 2015) and is divided into the following chapters in the training module: **Chapter 1** explains the specific user rights in the context of the European Union's General Data Protection Regulation (GDPR), for example, the right of access (§12) or the right to rectification of data (§16) (European Parliament, 2016). It clarifies users' rights regarding processing their personal data, such as the right to be informed about data use, the right to request corrections, and the right to withdraw consent. The chapter also discusses data protection regulations in international contexts, particularly concerning data transfers across borders and the necessary level of protection. **Chapter 2** highlights security gaps concerning IVAs and elucidates the legal ambiguities and abuses in which IVA providers frequently fail to comply with the current legal regulations. The issue is raised that smart speaker vendors may not provide sufficient information about data collection and use and may store personal data longer than the law permits, for example, due to inconsistencies in international data protection agreements. **Chapter 3** addresses data protection outside Europe, focusing on the Cloud Act and its potential risks to the secure transfer of European users' data to the USA. It explains how the

[2] Training Module 2: https://motiv.professor-x.de/train/PV3_v1.8JS.zip/index.html.

Table 1
Descriptive and inferential statistical evaluation results for Training Module 1.

	Pre		Post		Statistic				Effect Size
	M	SD	M	SD	t-value		df	p [a]	d
Privacy Aspects									
Subjective Privacy Literacy	3.23	0.85	3.56	0.66	−2.55	*	35	.014	−0.43
Privacy Concern: Device	3.39	0.81	3.61	0.92	−1.74	†	35	.051	−0.29
Privacy Concern: Stranger	3.14	1.05	3.40	1.04	−1.77	†	35	.051	−0.30
Privacy Concern: Company	3.44	0.76	3.70	0.84	−2.74	*	35	.010	−0.46
Trust	2.89	0.85	2.32	1.02	5.29	**	35	.005	0.88
Self-Disclosure	2.79	0.88	2.48	0.92	2.74	*	35	.010	0.46
Privacy Awareness	3.34	0.88	3.52	0.77	−1.86	*	35	.049	−0.31
Privacy Control	2.62	1.00	2.52	0.96	0.68		35	.751	0.11
Usage Aspects									
Ease of use	4.26	0.52	4.13	0.64	1.72	†	35	.051	0.29
Enjoyment	3.69	0.82	3.46	0.79	3.13	**	35	.007	0.52
Intention to use	4.15	0.94	3.81	1.07	2.82	*	35	.010	0.47
Social Perception									
Social-anthropomorphic	3.22	0.94	2.85	1.14	3.48	**	35	.005	0.58
Self-Determined Interaction									
Reflection	3.64	0.57	3.81	0.57	−2.12	*	35	.031	−0.35
Indulgence	3.76	0.72	3.27	0.97	3.55	**	35	.005	0.59

Note. [a] corrected *p*-values. †$p < .10$. *$p < .05$. **$p < .01$. ***$p < .001$.

Cloud Act allows US authorities to access data stored abroad, raising concerns about data protection. The training module contains single-choice and matching task exercises (examples in Table A1).

5.2. Participants

The sample consisted of $N = 33$ participants ($n_{\text{male}} = 14$, $n_{\text{female}} = 19$) recruited from the Prolific Panel. The mean age was 30.18 years ($SD = 9.57$, range = 19–67) (cf. Table A3). The same filters from Study 1 (Section 4.2) were applied, and another filter ensured that participants were excluded from the study for Training Module 2 if they had previously participated in Training Module 1. The majority of participants reported using IVAs daily (never = 0%; less than monthly = 9%; monthly = 12%; 2–3 times per month = 9%; weekly = 12%; 2–3 times per week = 12%; daily = 45%). Participants received monetary compensation (£8.92/h).

5.3. Measures

The measurement tools described in Section 3.2 were used to evaluate the effectiveness of the training module.

5.4. Results

The results of the analysis can be found in Table 2. Contrary to expectations, the training did not affect *subjective privacy literacy* and *privacy concerns* regarding strangers and companies. However, the training significantly increased *privacy concerns* regarding the device. As predicted, the training decreased *trust* marginally significantly. Contrary to prediction, the training did not impact the willingness to *self-disclose*. As expected, the training had a marginally significant positive effect on *privacy awareness* and *control*. In contrast to the hypothesis, the training had no significant effect on *ease of use*, *enjoyment*, or *intention to use*. In social perception, the training negatively affects the *social-anthropomorphic perception* of IVAs, as expected. Contrary to expectations, the training did affect *reflection* or *indulgence* in the domain of self-determined interaction. The criteria for adequate *training quality* were met: Subjective Fun ($M = 4.08$, $SD = 0.69$), Perceived Usefulness ($M = 4.11$, $SD = 0.69$), Perceived Difficulty ($M = 4.27$, $SD = 0.55$), Subjective Knowledge Growth ($M = 3.99$, $SD = 0.73$) and Attitude towards Training ($M = 4.11$, $SD = 0.72$).

Table 2
Descriptive and inferential statistical evaluation results for Training Module 2.

	Pre		Post		Statistic				Effect Size
	M	SD	M	SD	t-value		df	p [a]	d
Privacy Aspects									
Subjective Privacy Literacy	3.85	0.75	3.62	0.69	−0.37		32	.418	−0.06
Privacy Concern: Device	3.27	0.83	3.55	0.66	−2.62	**	32	.049	−0.46
Privacy Concern: Stranger	3.36	1.08	3.53	0.86	−1.27		32	.166	−0.22
Privacy Concern: Company	3.42	0.81	3.61	0.82	−1.30		32	.166	−0.23
Trust	3.05	0.98	2.85	0.95	2.20	†	32	.070	0.38
Self-Disclosure	2.66	0.83	2.70	0.82	−0.36		32	.638	−0.06
Privacy Awareness	3.68	0.77	3.88	0.63	−2.10	†	32	.070	−0.37
Privacy Control	3.00	0.85	3.25	0.96	−2.04	†	32	.070	−0.35
Usage Aspects									
Ease of use	4.19	0.53	4.17	0.70	0.21		32	.490	0.04
Enjoyment	3.82	0.79	3.70	0.82	1.35		32	.166	0.24
Intention to use	4.21	0.82	4.15	0.76	0.51		32	.389	0.09
Social Perception									
Social-anthropomorphic	3.39	0.58	3.08	0.81	3.68	*	32	.014	0.64
Self-Determined Interaction									
Reflection	3.59	0.69	3.75	0.67	−1.72		32	.112	−0.30
Indulgence	3.38	0.89	3.31	1.00	0.57		32	.389	0.10

Note. [a] corrected *p*-values. †$p < .10$. *$p < .05$. **$p < .01$. ***$p < .001$.

5.5. Discussion

Training Module 2 explained user rights in the interaction with IVAs and raised awareness of existing security gaps. The training did not affect subjective privacy literacy (H1 not confirmed). Theoretical knowledge of usage rights in the IVA context may not be sufficient to promote privacy literacy. Regarding other studies, more practical approaches that teach concrete privacy strategies and relevant device settings may be more useful (Trepte et al., 2015). The training led to a reappraisal of privacy concerns regarding the device, but not about strangers or companies (H2 partially confirmed). Although the training was primarily focused on questionable processes on the part of data processors, concerns about the device increased. This suggests that the learning content may not have been specific enough, as concerns are more likely to be seen with the device than with the providers responsible for data processing by the device or the underlying system architecture. Future training should focus more on applying user rights and security gaps in the context of specific providers to address privacy concerns at the company level.

The training reduced trust in IVAs marginally significantly (H2a confirmed) but did not affect the intention to disclose personal information (H2b not confirmed). The negative effect on trust could be increased awareness of acute use risks, leading participants to view IVAs as less trustworthy. Despite the close link between trust and self-disclosure (Rodríguez-Priego, Porcu, Pena, & Almendros, 2023), Training Module 2 only reduced trust, not self-disclosure. A related study also demonstrated that the effects on trust and self-disclosure need not occur simultaneously (Markus et al., 2024b). The lack of effect on self-disclosure may be related to the absence of an effect of training on subjective privacy literacy. Indeed, increased privacy literacy can negatively affect self-disclosure (Dienlin & Metzger, 2016; Harborth & Pape, 2020; Liao et al., 2019). However, training positively impacts privacy awareness and control (H4a-b confirmed). Participants are made aware of and interested in data protection issues by highlighting data protection rights and security gaps.

The training did not influence ease of use, enjoyment, or intention to use (H5a-c not confirmed), which were already high in the pretest and possibly too strong to be influenced by the relatively short-term training on privacy regulations. According to other research, this may be because privacy policies are often ignored due to their complexity, are perceived as irrelevant, and do not influence usage behavior (Rudolph et al., 2018). The training resulted in a reduction in social anthropomorphic perceptions of IVAs (H6 confirmed). Consistent with other research, the increased awareness of the technical and legal limitations of IVAs could have promoted the understanding of IVAs as complex software programs and reduced the perception of IVAs as social beings (Van Straten, Peter, Kühne, & Barco, 2020, 2022, pp. 1–17). The training did not increase the intention to use IVAs reflectively, nor did it decrease indulgence toward them (H7a-b not confirmed). This indicates that the training does not create a sufficiently broad knowledge base to support reflection in the context of own IVA usage (Hatlevik, 2012; Kember, 2008). Maybe it would be beneficial to include some practical examples of the application of user rights in the training to underline the high relevance for users, increasing reflection (Petty & Cacioppo, 1986). Regarding indulgence, the association of the training topic with neutral or positive emotions may not have negatively influenced indulgence toward IVAs (Cho et al., 2020; McCullough, 2000), creating favorable conditions for self-determined IVA interactions (Carolus, Augustin, et al., 2023).

6. General discussion

This study presents two self-developed privacy literacy training modules (Training Module 1: "Institutional Practices"; Training Module 2: "User Rights and Security Gaps"), designed using instructional psychology principles to foster positive learning experiences. The modules are grounded in the Digital Interaction Literacy Model (Carolus, Augustin, et al., 2023), which provides a competency framework and addresses the learning needs for self-determined and competent interaction with intelligent voice assistants. The modules' effects on privacy, usage patterns, social perceptions, and self-determined interaction were evaluated, with the results summarized in Table 3.

Training Module 1 positively affected subjective privacy literacy compared to Training Module 2. The understanding of how IVA providers process and market usage data (Training Module 1) seems more relevant for developing higher subjective privacy literacy than the content of Training Module 2, which addresses the user rights in the interaction with IVAs. Nevertheless, research indicates that understanding user rights is crucial for developing privacy literacy (Prince et al., 2024). Therefore, alternative training approaches should be found to replicate these findings. For example, instructional videos could illustrate the implementation of privacy policies in the context of IVAs, making learning more practical and relevant. In this way, theoretical knowledge about users' rights could be expanded in practice, positively related to privacy literacy (Desimpelaere et al., 2020). Furthermore, both training modules increased privacy concerns about the device. Training Module 1 additionally increased privacy concerns about strangers and IVA providers marginally significantly. This may be because Training Module 1 addressed privacy issues at all these stakeholder levels compared to Training Module 2. On the other hand, the missing effect of Training Module 2 on the other levels of privacy concerns may also be related to the lack of effectiveness of training on subjective privacy literacy. For example, Desimpelaere et al. (2020) found that people with higher privacy literacy had more negative attitudes towards data processors. Regarding trust, Trainings Modul 1 reduces trust in IVAs significantly and Trainings Modul 2 marginally significantly. According to other studies, the training may have violated privacy expectations and reduced IVA providers' perceived respect for privacy, which could explain the negative effect on trust (Lauer & Deng, 2007; Martin, 2018). In terms of self-disclosure, Training Module 1 significantly reduced self-disclosure, but Training Module 2 did not. To reduce learners' willingness to disclose personal data, a new training approach should be adopted for Training Module 2. In line with other studies, user rights could be more closely linked to the risks of disclosing personal data, which reduces the willingness to self-disclose (Joinson, Paine, Buchanan, & Reips, 2008). Training Module 1 and, tendentially, Training Module 2 were able to increase privacy awareness and thus interest in privacy issues. However, a trend towards a positive effect on perceived privacy control was only observed in Training Module 2. Training Module 1, which focused primarily on the commercialization of IVAs and the potential for privacy violations, may have raised awareness of the difficulty of privacy control, which consequently did not have a positive effect. In contrast, Training Module 2 provides the

Table 3
Overview of the confirmed (✓) and unconfirmed (X) hypotheses of the study.

Hypotheses			TM 1: Institutional Practices	TM 2: User Rights and Security Gaps
1	Increasing	Subjective Privacy Literacy	✓	X
2	Increasing	Privacy Concerns	✓	✓ (partly)
3	Reducing	a) Trust	✓	✓
		b) Self-Disclosure	✓	X
4	Increasing	a) Privacy Awareness	✓	✓
		b) Privacy Control	X	✓
5	Reducing	a) Ease of use	✓	X
		b) Enjoyment	✓	X
		c) Intention to use	✓	X
6	Reducing	Social-Anthropomorphic Perception	✓	✓
7	Increasing	a) Reflection	✓	X
	Reducing	b) Indulgence	✓	X

Note. TM = Training Module.

legal approaches for securing one's privacy, which, according to other studies, also led participants to develop higher perceived privacy control (Boerman, Strycharz, & Smit, 2024).

Compared to Training Module 2, Training Module 1 negatively affects the usage variables enjoyment, intention to use and tends to impact ease of use as well. This can be attributed to the increased focus on privacy risks in Training Module 1. Consistent with other studies, perceived privacy risks can reduce the enjoyment and intention to use AI-based technologies, while uncertainty about the security of one's privacy negatively affects ease of use (Ernst & Ernst, 2016; Martínez-Navalón, Fernández-Fernández, & Alberto, 2023). Both trainings reduce the social-anthropomorphic perception of IVAs. The reason for this could be the presentation of privacy risks and data protection gaps in the training, which could affect the sense of security and the associated perceived controllability towards IVAs. However, this is a favorable prerequisite for perceiving technology as anthropomorphic (Bartneck, Kulić, Croft, & Zoghbi, 2009; Blut, Wang, Wünderlich, & Brock, 2021; Epley, Waytz, & Cacioppo, 2007). Only Training Module 1 increased the intention to interact more reflectively with IVAs and affected indulgence negatively, as predicted. The mere explanation of user rights and security vulnerabilities (Training Module 2) may not be sufficient and should be supplemented by practical examples relevant to learners, as perceived self-reference can promote reflection (Petty & Cacioppo, 1986). In addition, legal texts, as in Training Module 2, tend to be written in a factual and value-free manner, which may have led learners to perceive the content as neutral and less negative. This may have prevented the negative training effect on indulgence that occurs when content is associated with negative emotions (Cho et al., 2020; McCullough, 2000).

Overall, both training modules effectively actualize device privacy concerns and trust in IVAs. In addition, Training Module 1 increases subjective privacy literacy, tends to affect privacy concerns for the "company" and "strangers" domains, and reduces the intention to disclose personal information to IVAs. Furthermore, both training modules promote privacy awareness, while Training Module 2 also tends to increase perceived privacy control. Training Module 1 promotes reevaluating usage acceptance variables by reducing ease of use, enjoyment, and intention to use IVAs. In addition, the training reduces social anthropomorphic perceptions, which are often associated with usage risks (Gaiser & Utz, 2023; Voorveld & Araujo, 2020; Wienrich et al., 2021). Training Module 1 also shows that presenting institutional practices by IVA providers and associated risks can increase reflectively IVA usage and reduce indulgence towards IVAs. Results also suggest that in addition to the content-based validity of the training modules through the Digital Interaction Literacy Model, they also demonstrate construct validity through the positive impact on Privacy Literacy and internal validity due to the high quality of the training modules. Overall, the training modules complement each other and fit holistically into an effective training program to strengthen users' privacy literacy and counteract negative privacy consequences in the context of IVAs.

6.1. Implications

The developed training modules and the selected training approach effectively promote privacy literacy in the context of IVAs and support literate interaction with them. From a privacy perspective, the training modules provide a basis for reassessing and evaluating privacy concerns at relevant stakeholder levels, including the device, stranger, and company. The modules promote the reflective use of IVAs and foster greater privacy awareness, privacy-related control beliefs, and privacy-friendly behaviors. These changes could lead to usage adaptation and privacy-friendly behaviors, which are crucial for self-determined interaction with IVAs (Carolus, Augustin, et al., 2023; Prince et al., 2024). The learners' positive evaluations of the training quality strengthen the training modules' validity and confirm the effectiveness of the instructional design. Consistent with previous research, these evaluations suggest that the training outcomes were not biased by negative learning experiences, such as perceived low usefulness or unfavorable attitudes toward the training (Joo, Lim, & Kim, 2013; NOE & Wilk, 1993; Schunk, 2005; Tannenbaum, Mathieu, Salas, & Cannon-Bowers, 1991). In addition, the online format of the training modules makes them accessible to diverse audiences, promoting broad social participation and reducing the digital divide. The success of the training approach suggests pedagogical potential that could be applied to increasingly important AI-related skills, such as understanding algorithms or using voice-based AI systems effectively (Carolus, Augustin, et al., 2023). Educational institutions could integrate the training modules into their curricula and adapt them to specific target groups to strengthen digital skills in a targeted manner. The modules are particularly valuable for older people with physical limitations or visual impairments, who can achieve more autonomy and active participation in the digital society through IVAs (Vieira, Leite, & Volochtchuk, 2022). The training modules help to improve the quality of life of these people by raising the level of privacy and awareness in the use of IVAs. They also promote access to reflections on possible concerns, intentions of use, and the consequences of anthropomorphization when interacting with IVAs. Digital transformation brings opportunities and challenges to society, so improving digital interaction skills, including privacy literacy, is essential (Carolus, Augustin, et al., 2023). Training in this area supports the empowered and self-determined use of voice-based AI systems, minimizes misunderstandings, and strengthens the ability to protect one's privacy. The training modules developed thus provide a basis for further training approaches to educate and support different people to become informed users of the digital technology landscape. In this way, they can help to better control the perceived risks according to their own usage needs, protect personal data according to their own wishes and make self-determined decisions about their disclosure.

The effectiveness of the privacy literacy training modules could be further enhanced by integrating educational theory approaches. Constructivism emphasizes that learning is an active, individual process in which new knowledge is created by linking it to existing experiences (Bada & Olusegun, 2015; Bereiter, 1994; Von Glasersfeld, 2013). Based on this, personalized learning experiences could be incorporated into online training, such as AI-based feedback systems that specifically repeat topics or exercises in which learners showed weaknesses after a learning session, thus promoting active learning and self-assessment. Behavioristic principles can be used in instructional design to reinforce desired behavior (Ertmer & Newby, 2013), for example, through rewards such as badges for completing modules or achieving high exercise scores. Another promising practical implication would be offering the developed privacy training modules on an open platform, which could be combined with other training to promote digital interaction literacy. Connectivism highlights the importance of networks in rapidly disseminating knowledge (Siemens, 2005), supporting collaborative learning and knowledge acquisition, as shown in studies Massive Open Online Courses (Mackness, Mak, & Williams, 2010). Integrating connectivist principles into an open online training platform could foster collaborative learning, allowing learners to co-develop privacy-friendly routines for everyday IVA use, thus encouraging social exchange and practical learning. We recommend developing practical concepts for integrating collaborative learning environments in future studies to optimize and broaden the accessibility of training. Additionally, gamification-based educational approaches could effectively combine the strengths of behaviorism, constructivism, and connectivism - reinforcing behaviorism with rewards like points and badges, supporting constructivism through interactive and problem-solving tasks, and promoting connectivism with collaborative, competitive elements such as leaderboards and team challenges that encourage knowledge sharing and networking (Costello, 2020).

6.2. Limitations and future directions

The sample studied represents a demographic cross-section of middle-aged people who are relatively frequent users of and familiar with IVAs. However, the sample size is relatively small. Increasing the sample size could enhance statistical power, improve the reliability of the findings, and broaden the generalizability of the results. The specificity of the sample makes it difficult to generalize the findings, suggesting that future research should account for a wider range of demographic factors, such as age, usage patterns, socioeconomic status, and device ownership. Research suggests that gender and educational level could influence training outcomes and needs. For example, men tend to have more positive attitudes toward AI technologies, while people with lower levels of education tend to have more negative perceptions. This could indicate that adapted training approaches are needed to achieve comparable training effects (Czaja et al., 2006; Gnambs & Appel, 2019; Rice, Winter, Mehta, & Ragbir, 2019; Stöhr, Ou, & Malmström, 2024). Furthermore, according to Meier and Krämer (2024), men and individuals with education levels tend to have fewer privacy concerns and higher privacy literacy, indicating that training content may need to be adapted to account for gender and educational background. In this context, a heterogeneous sample composition enables a more nuanced analysis to identify specific training needs for different target groups (e.g., young people using IVAs on smartphones; adults interacting with voice-based AI systems in their daily work) and potential variations in training outcomes. For instance, older individuals tend to be more skeptical about data processing and sharing compared to younger generations, who are more accustomed to the constant use of digital media and data sharing (e.g., on social media) (Bonilla & Martin-Hammond, 2020; Courtney, 2017). In particular, older adults and people with visual impairments find IVAs particularly useful (Vieira et al., 2022), highlighting the need to consider these populations in future intervention studies. Consideration should be given to adapting training materials to the needs of the target groups, for example, by providing larger font sizes or audio content optimized for older learners.

In addition, longitudinal studies offer the opportunity to evaluate the long-term effects of training, to track changes in user behavior over time (e.g., frequency of use, type of features used), and to derive further training optimizations in terms of long-term effects. A more detailed analysis of the training elements can also be performed to understand which specific training components led to the observed effects, providing the basis for further optimization. In this study, participants' exercise performance was not explicitly tracked, as these were mainly used to actively engage them in the learning material and internalize learning content (Wilder et al., 2001; Zarei, 2013). However, in future studies, exercise performance could provide a more objective measure of acquired privacy literacy, enabling a more accurate assessment of training effectiveness on variables such as user behavior and privacy perceptions. To further develop Training Module 2, we recommend integrating learning videos showing privacy-optimizing practical implementations of user rights within the device settings to strengthen subjective privacy literacy with practical relevance. Furthermore, this work examined training effects on subjectively perceived privacy literacy, but research shows that subjective and objective privacy literacy is not necessarily correlated (Ma & Chen, 2023). Future research approaches should, therefore, go beyond subjective perceptions and measure privacy literacy based on more objective and behavioral indicators, such as privacy settings made in devices or the type and frequency of personal data disclosure. In addition, the results suggest that indulgence towards IVAs decreases after Training Module 1. However, as appropriate indulgence is recommended for self-determined interaction (Carolus, Augustin, et al., 2023; Schweitzer et al., 2019), training components that increase indulgence may be advisable. Markus et al. (2024b) showed that indulgence toward IVAs increases when users understand how they work and process voice commands technically, as well as potential sources of mistakes. In privacy literacy training, indulgence could be generated by explaining why IVAs need certain personal data (e.g., to offer a wide function range) while providing learners practical tips for monitoring and adjusting data activity.

6.3. Conclusion

In this work, two privacy literacy training modules were developed and tested for their effectiveness concerning aspects of privacy, usage, social perception, and self-determined interaction. The first training module showed a significant improvement in subjective privacy literacy and an adjustment in usage perceptions, while the second module tended to increase users' perceived privacy control. Both trainings led to a reassessment of privacy concerns, reduced trust, and a decreased social-anthropomorphic perception of IVAs. Training Module 1 also increased the intention to use IVAs reflectively, which is important for self-determined interaction with these systems. Overall, the two training modules offer a comprehensive solution for strengthening privacy literacy and minimizing negative privacy consequences in IVA use. They are suitable for integration into educational institutions to promote digital interaction literacy and are particularly valuable for vulnerable populations. These training modules contribute to developing AI-related skills that will be indispensable in a world where AI increasingly permeates everyday life. They promote conscious and self-determined behavior in dealing with AI and thus have the potential to strengthen skills in dealing with AI in everyday life.

CRediT authorship contribution statement

André Markus: Writing – review & editing, Writing – original draft, Visualization, Validation, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Maximilian Baumann:** Writing – review & editing, Writing – original draft, Software, Methodology, Investigation, Conceptualization. **Jan Pfister:** Validation, Software, Investigation, Data curation, Conceptualization. **Astrid Carolus:** Writing – review & editing, Supervision, Resources, Project administration, Funding acquisition, Conceptualization. **Andreas Hotho:** Resources, Project administration, Funding acquisition. **Carolin Wienrich:** Writing – review & editing, Supervision, Resources, Project administration, Funding acquisition, Conceptualization.

Data availability

The data underlying this article will be shared at a reasonable request by the corresponding author.

Ethical statement

The procedure performed in this study was conducted in accordance with the ethical standards outlined in the 1964 Declaration of Helsinki and its later amendments. An ethical review and approval were not required for the study of human participants in accordance with institutional requirements. The study did not involve medical, biological, personal, or sensitive data requiring specific ethical approval. All standard procedures to minimize risks for participants were strictly followed, including adherence to ethical guidelines for data collection. Informed consent was obtained from the participants to participate in the current study.

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.

Acknowledgments

We thank our research assistants Jule Puchner, Pascal Jeck and Johannes Aumiller for their support in the technical and content-related creation of the training modules. This research was funded by the German Federal Ministry of Labour and Social Affairs [DKI.00.00030.21].

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.caeai.2025.100372.

References

Abdi, N., Zhan, X., Ramokapane, K., & Such, J. (2021). *Privacy norms for smart home personal assistants Proceedings of the 2021 CHI conference on human factors in computing systems*. New York: US.

Adobe, C. (2019). Adobe captivate classic (version 11). *Adobe Systems*. https://www.adobe.com/products/captivate/captivate-classic.html.

Agrawal, A., Gans, J., & Goldfarb, A. (2018). Google's AI assistant is a reminder that privacy and security are not the same. Retrieved June 20 from https://hbr.org/2018/05/googles-ai-assistant-is-a-reminder-that-privacy-and-security-are-not-the-same.

Alliger, G. M., Tannenbaum, S. I., Bennett Jr, W., Traver, H., & Shotland, A. (1997). A meta-analysis of the relations among training criteria. *Personnel Psychology, 50*(2), 341–358. https://doi.org/10.1111/j.1744-6570.1997.tb00911.x

Angst, C., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly*, 339–370. https://doi.org/10.2307/20650295

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304–312. https://doi.org/10.1016/j.chb.2014.05.046

Aron, A., Aron, E., & Coups, E. (2014). *Statistics for psychology (6. uppl.)*. Boston, US: Pearson.

Bada, S. O., & Olusegun, S. (2015). Constructivism learning theory: A paradigm for teaching and learning. *Journal of Research & Method in Education, 5*(6), 66–70.

Bandyopadhyay, S. (2012). Consumers' online privacy concerns: Causes and effects. *Innovative Marketing, 8*(3), 32–39. https://doi.org/10.19030/iber.v10i2.1797

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. https://doi.org/10.1007/s12369-008-0001-3

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior, 56*, 147–154. https://doi.org/10.1016/j.chb.2015.11.022

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Benjamini, Y., & Hochberg, Y. (1995). Controlling the false discovery rate: A practical and powerful approach to multiple testing. *Journal of the Royal Statistical Society: Series B, 57*(1), 289–300. https://doi.org/10.1111/j.2517-6161.1995.tb02031.x

Bereiter, C. (1994). Constructivism, socioculturalism, and Popper's world 3. *Educational Researcher, 23*(7), 21–23. https://doi.org/10.2307/1176935

Blut, M., Wang, C., Wünderlich, N. V., & Brock, C. (2021). Understanding anthropomorphism in service provision: A meta-analysis of physical robots, chatbots, and other AI. *Journal of the Academy of Marketing Science, 49*, 632–658. https://doi.org/10.1007/s11747-020-00762-y

Boerman, S., Kruikemeier, S., & Zuiderveen Borgesius, F. (2021). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research, 48*(7), 953–977. https://doi.org/10.1177/0093650218800915

Boerman, S., Strycharz, J., & Smit, E. (2024). How can we increase privacy protection behavior? A longitudinal experiment testing three intervention strategies. *Communication Research, 51*(2), 115–145. https://doi.org/10.1177/00936502231177786

Bonilla, K., & Martin-Hammond, A. (2020). Older adults' perceptions of intelligent voice assistant privacy, transparency, and online privacy guidelines. *Sixteenth symposium on useable privacy and security (SOUPS 2020)*. Boston: US.

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: The importance of internet skills for online privacy protection. *Information, Communication & Society, 20*(8), 1261–1278. https://doi.org/10.1080/1369118X.2016.1229001

Carolus, A., Augustin, Y., Markus, A., & Wienrich, C. (2023). Digital interaction literacy model: Conceptualizing competencies for literate interactions with voice-based AI systems. *Computers & Education: Artificial Intelligence, 4*, Article 100114. https://doi.org/10.1016/j.caeai.2022.100114

Carolus, A., Koch, M., Straka, S., Latoschik, M. E., & Wienrich, C. (2023). MAILS-Meta AI literacy scale: Development and testing of an AI literacy questionnaire based on well-founded competency models and psychological change-and meta-competencies. *Computers in Human Behavior: Artificial Humans, 1*(2), Article 100014. https://doi.org/10.1016/j.chbah.2023.100014

Cespedes, F., & Smith, J. (1993). Database marketing: New rules for policy and practice. *MIT Sloan Management Review, 34*(4), 7–22.

Chetty, K., Qigui, L., Gcora, N., Josie, J., Wenwei, L., & Fang, C. (2018). Bridging the digital divide: Measuring digital literacy. *Economics, 12*(1), 1–20.

Cheung, A. C., & Slavin, R. E. (2013). The effectiveness of educational technology applications for enhancing mathematics achievement in K-12 classrooms: A meta-analysis. *Educational Research Review, 9*, 88–113. https://doi.org/10.1016/j.edurev.2013.01.001

Cho, H., Li, P., & Goh, Z. H. (2020). Privacy risks, emotions, and social media: A coping model of online privacy. *ACM Transactions on Computer-Human Interaction, 27*(6), 1–28. https://doi.org/10.1145/3412367

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

Clark, R., & Mayer, R. (2016). *E-Learning and the science of instruction: Proven guidelines for consumers and designers of multimedia learning*. John Wiley & Sons.

Cobb, C., Bhagavatula, S., Garrett, K. A., Hoffman, A., Rao, V., & Bauer, L. (2021). "I would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users. *Proceedings on privacy enhancing technologies*.

Costello, R. (2020). Learning theories within gamification. In R. Costello (Ed.), *Gamification strategies for retention, motivation, and engagement in higher education: Emerging research and opportunities* (pp. 1–61). IGI Global. https://doi.org/10.4018/978-1-7998-2079-6.ch001.

Couper, M., Tourangeau, R., & Steiger, D. (2001). *Social presence in web surveys Proceedings of the SIGCHI conference on Human factors in computing systems*. New York: US.

Courtney, M. (2017). Careless talk costs privacy [digital assistants]. *Engineering & Technology, 12*(10), 50–53. https://doi.org/10.1049/et.2017.1005

Czaja, S. J., Charness, N., Fisk, A. D., Hertzog, C., Nair, S. N., Rogers, W. A., et al. (2006). Factors predicting the use of technology: Findings from the center for research and education on aging and technology enhancement (CREATE). *Psychology and Aging, 21*(2), 333–352.

de Kloet, M., & Yang, S. (2022). The effects of anthropomorphism and multimodal biometric authentication on the user experience of voice intelligence. *Frontiers in Artificial Intelligence, 5*, Article 831046. https://doi.org/10.3389/frai.2022.831046

Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in Human Behavior, 110*, Article 106382. https://doi.org/10.1016/j.chb.2020.106382

Dienlin, T., & Metzger, M. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. *Journal of Computer-Mediated Communication, 21*(5), 368–383. https://doi.org/10.1111/jcc4.12163

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. https://doi.org/10.2753/JEC1086-4415100201

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Eastlick, M. A., Lotz, S., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research, 59*(8), 877–886. https://doi.org/10.1016/j.jbusres.2006.02.006

Easwara Moorthy, A., & Vu, K.-P. (2014). *Voice activated personal assistant: Acceptability of use in the public space* human interface and the management of information. *Information and knowledge in applications and services: 16th international conference, heraklion, crete, Greece*.

Edu, J., Such, J., & Suarez-Tangil, G. (2020). Smart home personal assistants: A security and privacy review. *ACM Computing Surveys, 53*(6), 1–36. https://doi.org/10.1145/3412383

Emami-Naeini, P., Dixon, H., Agarwal, Y., & Cranor, L. F. (2019). Exploring how privacy and security factor into IoT device purchase behavior. *Proceedings of the 2019 CHI conference on human factors in computing systems*. New York: US.

Epley, N., Waytz, A., & Cacioppo, J. (2007). On seeing human: A three-factor theory of anthropomorphism. *Psychological Review, 114*(4), 864–886. https://doi.org/10.1037/0033-295X.114.4.864

Ernst, C.-P., & Ernst, A. (2016). *The Influence of privacy Risk on smartwatch usage twenty-second americas conference on information systems*. San Diego, CA.

Ertmer, P. A., & Newby, T. J. (2013). Behaviorism, cognitivism, constructivism: Comparing critical features from an instructional design perspective. *Performance Improvement Quarterly, 26*(2), 43–71. https://doi.org/10.1002/piq.21143

European Data Protection Board. (2021). Guidelines 02/2021 on virtual voice assistants. Retrieved June 20 from https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-022021-virtual-voice-assistants_en.

European Parliament. (2016). General data protection regulation (GDPR). Retrieved June, 20 from https://dsgvo-gesetz.de/.

Faul, F., Erdfelder, E., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods, 39*, 175–191.

Fowler, G. (2018). "I live with Alexa, Google Assistant and Siri. here's which one you should pick. *Washington Post*. Retrieved June 20 from https://www.washingtonpost.com/technology/2018/11/21/i-live-with-alexa-google-assistant-siri-heres-which-you-should-pick/.

Gaiser, F., & Utz, S. (2023). Is hearing really believing? The importance of modality for perceived message credibility during information search with smart speakers. *Journal of Media Psychology: Theories, Methods, and Applications*, 93–106. https://doi.org/10.1027/1864-1105/a000384

Gardiner, B. (2018). Private smarts–can digital assistants work without prying into our lives. *Scientific American*. Retrieved June 20 from https://www.scientificamerican.com/article/private-smarts-can-digital-assistants-work-without-prying-into-our-lives/.

Gegenfurtner, A. (2011). Motivation and transfer in professional training: A meta-analysis of the moderating effects of knowledge type, instruction, and assessment conditions. *Educational Research Review, 6*(3), 153–168. https://doi.org/10.1016/j.edurev.2011.04.001

Gilbert, J. (2001). Privacy? Who needs privacy. *Business, 2*(6), 2.

Gnambs, T., & Appel, M. (2019). Are robots becoming unpopular? Changes in attitudes towards autonomous robotic systems in Europe. *Computers in Human Behavior, 93*, 53–61. https://doi.org/10.1016/j.chb.2018.11.045

Goldstein, I., & Ford, J. K. (2002). *Training in organizations* (4 ed.). Wadsworth/Thomson Learning.

González-Rodríguez, J., Toledano, D. T., & Ortega-García, J. (2008). Voice biometrics. In *Handbook of biometrics* (pp. 151–170). Springer. https://doi.org/10.1007/978-0-387-71041-9_8.

Guidi, A., Gentili, C., Scilingo, E. P., & Vanello, N. (2019). Analysis of speech features and personality traits. *Biomedical Signal Processing and Control, 51*, 1–7. https://doi.org/10.1016/j.bspc.2019.01.027

Gupta, P., Hooda, A., Jeyaraj, A., Seddon, J. J., & Dwivedi, Y. K. (2024). Trust, risk, privacy and security in e-Government use: Insights from a MASEM analysis. *Information Systems Frontiers*, 1–17. https://doi.org/10.1007/s10796-024-10497-8

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior, 68*, 217–227. https://doi.org/10.1016/j.chb.2016.11.033

Harborth, D., & Pape, S. (2020). How privacy concerns, trust and risk beliefs, and privacy literacy influence users' intentions to use privacy-enhancing technologies: The case of Tor. *ACM SIGMIS - Data Base: The DATABASE for Advances in Information Systems, 51*(1), 51–69. https://doi.org/10.1145/3380799.3380805

Hasan, B. (2007). Examining the effects of computer self-efficacy and system complexity on technology acceptance. *Information Resources Management Journal, 20*(3), 76–88. https://doi.org/10.4018/irmj.2007070106

Hatlevik, I. K. R. (2012). The theory-practice relationship: Reflective skills and theoretical knowledge as key factors in bridging the gap between theory and practice in initial nursing education. *Journal of Advanced Nursing, 68*(4), 868–877. https://doi.org/10.1111/j.1365-2648.2011.05789.x

Heerink, M., Krose, B., Evers, V., & Wielinga, B. (2009). *Measuring acceptance of an assistive social robot: A suggested toolkit RO-MAN 2009-the 18th IEEE international symposium on robot and human interactive communication*. Toyama, Japan.

Hinde, S. (1998). Privacy and security—the drivers for growth of E-Commerce. *Computers & Security, 17*(6), 475–478. https://doi.org/10.1016/S0167-4048(98)80069-2

Huang, R. H., Han, Q., & Zhu, X. (2021). Protecting data privacy for mobile payments under the Chinese law: Comparative perspectives and reform suggestions. *Chi.-Kent J. Intell. Prop., 20*, 226.

Hwang, Y., & Kim, D. (2007). Customer self-service systems: The effects of perceived Web quality with service contents on enjoyment, anxiety, and e-trust. *Decision Support Systems, 43*(3), 746–760. https://doi.org/10.1016/j.dss.2006.12.008

Ischen, C., Araujo, T., Voorveld, H., van Noort, G., & Smit, E. (2020). *Privacy concerns in chatbot interactions chatbot research and design: Third international workshop, CONVERSATIONS 2019*. Amsterdam, Netherlands.

Jacobsson, A., & Davidsson, P. (2015). *Towards a model of privacy and security for smart homes* 2015. *IEEE 2nd World Forum on Internet of Things (WF-IoT)*. Milan, Italy.

Jayatilleke, A., Thelijjagoda, S., & Pathirana, P. (2019). Security awareness among smart speaker users. *2019 national information technology conference (NITC)*. Colombo, Sri Lanka.

Joinson, A., Paine, C., Buchanan, T., & Reips, U.-D. (2008). Measuring self-disclosure online: Blurring and non-response to sensitive items in web-based surveys. *Computers in Human Behavior, 24*(5), 2158–2171. https://doi.org/10.1016/j.chb.2007.10.005

Joo, Y. J., Lim, K. Y., & Kim, J. (2013). Locus of control, self-efficacy, and task value as predictors of learning outcome in an online university context. *Computers & Education, 62*, 149–158. https://doi.org/10.1016/j.compedu.2012.10.027

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). *My data just goes everywhere": User mental models of the Internet and implications for privacy and security eleventh symposium on useable privacy and security*. Pittsburgh: US.

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. https://doi.org/10.1177/14614448211026

Kember, D. (2008). *Reflective teaching and learning in the health professions: Action research in professional education*. John Wiley & Sons. https://doi.org/10.1002/9780470690550

Ketelaar, P., & Van Balen, M. (2018). The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. *Computers in Human Behavior, 78*, 174–182. https://doi.org/10.1016/j.chb.2017.09.034

Kim, J. Y., Chung, N., & Ahn, K. M. (2014). Why people use social networking services in Korea: The mediating role of self-disclosure on subjective well-being. *Information Development, 30*(3), 276–287. https://doi.org/10.1177/0266666913489894

Langer, I., von Thun, F. S., & Tausch, R. (2019). *Sich verständlich ausdrücken*. Ernst Reinhardt Verlag.

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*. New York: US.

Lauer, T., & Deng, X. (2007). Building online trust through privacy practices. *International Journal of Information Security, 6*, 323–331. https://doi.org/10.1007/s10207-007-0028-8

Leiner, D. J. (2024). SoSci survey [Computer software] Version 3.5.02. https://www.soscisurvey.de.

Liao, C., Liu, C.-C., & Chen, K. (2011). Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electronic Commerce Research and Applications, 10*(6), 702–715. https://doi.org/10.1016/j.elerap.2011.07.003

Liao, Y., Vitak, J., Kumar, P., Zimmer, M., & Kritikos, K. (2019). *Understanding the Role of Privacy and Trust in intelligent personal assistant adoption 14th international conference*. iConference 2019, Washington, DC, USA.

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

Ma, S., & Chen, C. (2023). Are digital natives overconfident in their privacy literacy? Discrepancy between self-assessed and actual privacy literacy, and their impacts on privacy protection behavior. *Frontiers in Psychology, 14*, Article 1224168. https://doi.org/10.3389/fpsyg.2023.1224168

Mackness, J., Mak, S., & Williams, R. (2010). The ideals and reality of participating in a MOOC. *Proceedings of the 7th international conference on networked learning 2010*. Lancaster, UK.

Maier, C., Laumer, S., Weinert, C., & Weitzel, T. (2015). The effects of technostress and switching stress on discontinued use of social networking services: A study of facebook use. *Information Systems Journal, 25*(3), 275–308. https://doi.org/10.1111/isj.12068

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

Markus, A., Pfister, J., Carolus, A., Hotho, A., & Wienrich, C. (2024a). Effects of AI understanding-training on AI literacy, usage, self-determined interactions, and anthropomorphization with voice assistants. *Computers and Education Open, 6*, Article 100176. https://doi.org/10.1016/j.caeo.2024.100176

Markus, A., Pfister, J., Carolus, A., Hotho, A., & Wienrich, C. (2024b). Empower the user-The impact of functional understanding training on usage, social perception, and self-determined interactions with intelligent voice assistants. *Computers & Education: Artificial Intelligence, 6*, Article 100229. https://doi.org/10.1016/j.caeai.2024.100229

Martin, K. (2018). The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research, 82*, 103–116. https://doi.org/10.1016/j.jbusres.2017.08.034

Martínez-Navalón, J.-G., Fernández-Fernández, M., & Alberto, F. P. (2023). Does privacy and ease of use influence user trust in digital banking applications in Spain and Portugal? *The International Entrepreneurship and Management Journal, 19*(2), 781–803. https://doi.org/10.1007/s11365-023-00839-4

Mayer, R. (2014). Multimedia instruction. In M. Spector, D. Merrill, J. Elen, & M. Bishop (Eds.), *Handbook of research on educational communications and technology* (pp. 385–399). Springer.

Mayer, R., & Fiorella, L. (2014). 12 principles for reducing extraneous processing in multimedia learning: Coherence, signaling, redundancy, spatial contiguity, and temporal contiguity principles. In R. Mayer (Ed.), *The Cambridge handbook of multimedia learning* (Vol. 279, pp. 279–315). New York, NY: Cambridge University Press.

McCullough, M. (2000). Forgiveness as human strenght: Theory, measurement, and links to well-being. *Journal of Social and Clinical Psychology, 1*(9), 43–55.

Meade, A., & Craig, B. (2012). Identifying careless responses in survey data. *Psychological Methods, 17*(3), 437. https://doi.org/10.1037/a0028085

Meier, Y., & Krämer, N. C. (2024). Differences in access to privacy information can partly explain digital inequalities in privacy literacy and self-efficacy. *Behaviour & Information Technology*, 1–16. https://doi.org/10.1080/0144929X.2024.2349183

Memon, M. A., Ting, H., Cheah, J.-H., Thurasamy, R., Chuah, F., & Cham, T. H. (2020). Sample size for survey research: Review and recommendations. *Journal of Applied Structural Equation Modeling, 4*(2), i–xx. https://doi.org/10.47263/JASEM.4(2)01

Mesch, G. S. (2012). Is online trust and trust in social institutions associated with online disclosure of identifiable information online? *Computers in Human Behavior, 28*(4), 1471–1477. https://doi.org/10.1016/j.chb.2012.03.010

Miltgen, C. L., Popovič, A., & Oliveira, T. (2013). Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context. *Decision Support Systems, 56*, 103–114. https://doi.org/10.1016/j.dss.2013.05.010

Monteleone, S., van Bavel, R., Rodríguez-Priego, N., & Esposito, G. (2015). *Nudges to privacy behaviour: Exploring an alternative approach to privacy notices*. Institute for Prospective Technological Studies - Joint Research Centre - European Commission. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC96695/jrc96695.pdf.

Nass, C. I., & Brave, S. (2005). *Wired for speech: How voice activates and advances the human-computer relationship*. MIT Press.

Noe, R. A., & Wilk, S. L. (1993). Investigation of the factors that influence employees' participation in development activities. *Journal of Applied Psychology, 78*(2), 291–302. https://doi.org/10.1037/0021-9010.78.2.291

O'Brien, N., & Sohail, M. (2020). Infrequent use of AI-enabled personal assistants through the lens of cognitive dissonance theory. *HCI international 2020–late breaking posters: 22nd international conference*. Copenhagen, Denmark.

Olson, C., & Kemery, K. (2019). *Voice report: Consumer adoption of voice technology and digital assistants*. Microsoft. https://voicey.co.il/wp-content/uploads/2019/04/microsoft-report-2019.pdf.

Pagano, R. R. (1990). *Understanding statistics in the behavioral sciences*. West Publishing Co.

Pal, D., Arpnikanondt, C., & Razzaque, M. A. (2020). Personal information disclosure via voice assistants: The personalization–privacy paradox. *SN Computer Science, 1*, 1–17. https://doi.org/10.1007/s42979-020-00287-9

Pal, D., Arpnikanondt, C., Razzaque, M. A., & Funilkul, S. (2020). To trust or not-trust: Privacy issues with voice assistants. *IT professional, 22*(5), 46–53. https://doi.org/10.1109/MITP.2019.2958914

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. *Advances in Experimental Social Psychology, 19*, 123–205. https://doi.org/10.1016/S0065-2601(08)60214-2

Pradhan, A., Mehta, K., & Findlater, L. (2018). *Accessibility Came by accident": Use of voice-controlled intelligent personal assistants by people with disabilities proceedings of the 2018 CHI conference on human factors in computing systems*. Montreal, Canada.

Prince, C., Omrani, N., & Schiavone, F. (2024). Online privacy literacy and users' information privacy empowerment: The case of GDPR in Europe. *Information Technology & People, 37*(8), 1–24. https://doi.org/10.1108/ITP-05-2023-0467

Rey, G. D., Beege, M., Nebel, S., Wirzberger, M., Schmitt, T. H., & Schneider, S. (2019). A meta-analysis of the segmenting effect. *Educational Psychology Review, 31*, 389–419. https://doi.org/10.1007/s10648-018-9456-4

Rice, S., Winter, S. R., Mehta, R., & Ragbir, N. K. (2019). What factors predict the type of person who is willing to fly in an autonomous commercial airplane? *Journal of Air Transport Management, 75*, 131–138. https://doi.org/10.1016/j.jairtraman.2018.12.008

Ritzmann, S., Hagemann, V., & Kluge, A. (2014). The Training Evaluation Inventory (TEI)-evaluation of training design and measurement of training outcomes for predicting training success. *Vocations and Learning, 7*, 41–73. https://doi.org/10.1007/s12186-013-9106-4

Ritzmann, S., Hagemann, V., & Kluge, A. (2020). The training evaluation inventory (TEI) – evaluation of training design and measurement of training outcomes for predicting training success. *Vocations and Learning, 7*, 41–73. https://doi.org/10.1007/s12186-013-9106-4

Rodríguez-Priego, N., Porcu, L., Pena, M. B. P., & Almendros, E. C. (2023). Perceived customer care and privacy protection behavior: The mediating role of trust in self-disclosure. *Journal of Retailing and Consumer Services, 72*, Article 103284. https://doi.org/10.1016/j.jretconser.2023.103284

Rudolph, M., Feth, D., & Polst, S. (2018). *Why users ignore privacy policies–a survey and intention model for explaining user privacy behavior* Human-Computer Interaction. *Human issues: 20th international conference*. USA: Theories, Methods.

Sawilowsky, S. S., & Blair, R. C. (1992). A more realistic look at the robustness and type II error properties of the t test to departures from population normality. *Psychological Bulletin, 111*(2), 352. https://doi.org/10.1037/0033-2909.111.2.352

Schneider, S., Nebel, S., & Rey, G. D. (2016). Decorative pictures and emotional design in multimedia learning. *Learning and Instruction, 44*, 65–73. https://doi.org/10.1016/j.learninstruc.2016.03.002

Schön, D. (2017). *The reflective practitioner: How professionals think in action*. Routledge. https://doi.org/10.4324/9781315237473

Schunk, D. H. (2005). Self-regulated learning: The educational legacy of Paul R. Pintrich. *Educational Psychologist, 40*(2), 85–94. https://doi.org/10.1207/s15326985ep4002_3

Schweitzer, F., Belk, R., Jordan, W., & Ortner, M. (2019). Servant, friend or master? The relationships users build with voice-controlled smart devices. *Journal of Marketing Management, 35*(7–8), 693–715. https://doi.org/10.1080/0267257X.2019.1596970

Sciuto, A., Saini, A., Forlizzi, J., & Hong, J. (2018). Hey Alexa, what's up?. *A mixed-methods studies of in-home conversational agent usage Proceedings of the 2018 designing interactive systems conference, Hong Kong, China*.

Sharif, K., & Tenbergen, B. (2020). Smart home voice assistants: A literature survey of user privacy and security vulnerabilities. *Complex Systems Informatics and Modeling Quarterly*, (24), 15–30. https://doi.org/10.7250/csimq.2020-24.02

Shin, D., Zhong, B., & Biocca, F. (2020). Beyond user experience: What constitutes algorithmic experiences? *International Journal of Information Management, 52*, Article 102061. https://doi.org/10.1016/j.ijinfomgt.2019.102061

Sideri, M., Kitsiou, A., Tzortzaki, E., Kalloniatis, C., & Gritzalis, S. (2019). Enhancing university students' privacy literacy through an educational intervention: A Greek case-study. *International Journal of Electronic Governance, 11*(3–4), 333–360. https://doi.org/10.1504/IJEG.2019.103719

Siemens, G. (2005). Connectivism: A learning theory for the digital age. *International Journal of Instructional Technology and Distance Learning, 2*(1), 3–10.

Son, J.-Y., & Kim, S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, 503–529. https://doi.org/10.2307/25148854

Spanjers, I. A., Van Gog, T., & van Merriënboer, J. J. (2010). A theoretical analysis of how segmentation of dynamic visualizations optimizes students' learning. *Educational Psychology Review, 22*, 411–423. https://doi.org/10.1007/s10648-010-9135-6

Spatola, N., Kühnlenz, B., & Cheng, G. (2021). Perception and evaluation in human-robot interaction: The human–robot interaction evaluation scale (HRIES) - a multicomponent approach of anthropomorphism. *International journal of social robotics, 13*(7), 1517–1539. https://doi.org/10.1007/s12369-020-00667-4

Stöhr, C., Ou, A. W., & Malmström, H. (2024). Perceptions and usage of AI chatbots among students in higher education across genders, academic levels and fields of study. *Computers & Education: Artificial Intelligence, 7*, Article 100259. https://doi.org/10.1016/j.caeai.2024.100259

Storey, J. D. (2002). A direct approach to false discovery rates. *Journal of the Royal Statistical Society - Series B: Statistical Methodology, 64*(3), 479–498. https://doi.org/10.1111/1467-9868.00346

Suffoletto, B., Anwar, A., Glaister, S., & Sejdic, E. (2023). Detection of alcohol intoxication using voice features: A controlled laboratory study. *Journal of Studies on Alcohol and Drugs, 84*(6), 808–813. https://doi.org/10.15288/jsad.22-00375

Sulpizio, S., Fasoli, F., Maass, A., Paladino, M. P., Vespignani, F., Eyssel, F., et al. (2015). The sound of voice: Voice-based categorization of speakers' sexual orientation within and across languages. *PLoS One, 10*(7), Article e0128882. https://doi.org/10.1371/journal.pone.0128882

Sweller, J., van Merriënboer, J., & Paas, F. (2019). Cognitive architecture and instructional design: 20 years later. *Educational Psychology Review, 31*, 261–292. https://doi.org/10.1007/s10648-019-09465-5

Tabassum, M., Kosinski, T., & Lipford, H. R. (2019). I don't own the data. *End user Perceptions of smart home device data Practices and risks fifteenth symposium on useable privacy and security (SOUPS 2019)*. Santa Clara, US.

Tannenbaum, S. I., Mathieu, J. E., Salas, E., & Cannon-Bowers, J. A. (1991). Meeting trainees' expectations: The influence of training fulfillment on the development of commitment, self-efficacy, and motivation. *Journal of Applied Psychology, 76*(6), 759–769. https://doi.org/10.1037/0021-9010.76.6.759

Thielsch, M., & Hirschfeld, G. (2021). *Unaufmerksamkeit, Faking, Speedster… Kontrolle der Datenqualität in User Experience Befragungen Mensch und Computer*. Ingolstadt, Germany.

Thoret, E., Andrillon, T., Gauriau, C., Leger, D., & Pressnitzer, D. (2024). Sleep deprivation detected by voice analysis. *PLoS Computational Biology, 20*(2), Article e1011849. https://doi.org/10.1371/journal.pcbi.1011849

Trepte, S., Teutsch, D., Masur, P., Eicher, C., Fischer, M., Hennhöfer, A., et al. (2015). Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale"(OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law* (Vol. 20, pp. 333–365). Springer. https://doi.org/10.1007/978-94-017-9385-8_14.

Van Straten, C., Peter, J., Kühne, R., & Barco, A. (2020). Transparency about a robot's lack of human psychological capacities: Effects on child-robot perception and relationship formation. *ACM Transactions on Human-Robot Interaction (THRI), 9*(2), 1–22. https://doi.org/10.1145/3365668

Van Straten, C., Peter, J., Kühne, R., & Barco, A. (2022). *The wizard and I: How transparent teleoperation and self-description (do not) affect children's robot perceptions and child-robot relationship formation* (pp. 1–17). Ai & Society. https://doi.org/10.1007/s00146-021-01202-3

Vanderhoven, E., Schellens, T., & Valcke, M. (2016). Decreasing risky behavior on social network sites: The impact of parental involvement in secondary education interventions. *Journal of Primary Prevention, 37*, 247–261. https://doi.org/10.1007/s10935-016-0420-0

Vieira, A. D., Leite, H., & Volochtchuk, A. V. L. (2022). The impact of voice assistant home devices on people with disabilities: A longitudinal study. *Technological Forecasting and Social Change, 184*, Article 121961. https://doi.org/10.1016/j.techfore.2022.121961

Von Glasersfeld, E. (2013). *Radical constructivism*. Routledge. https://doi.org/10.4324/9780203454220

Voorveld, H., & Araujo, T. (2020). How social cues in virtual assistants influence concerns and persuasion: The role of voice and a human name. *Cyberpsychology, Behavior, and Social Networking, 23*(10), 689–696. https://doi.org/10.1089/cyber.2019.0205

Wang, L., Sun, Z., Dai, X., Zhang, Y., & Hu, H.-h. (2019). Retaining users after privacy invasions: The roles of institutional privacy assurances and threat-coping appraisal in mitigating privacy concerns. *Information Technology & People, 32*(6), 1679–1703. https://doi.org/10.1108/ITP-01-2018-0020

Warr, P., Allan, C., & Birdi, K. (1999). Predicting three levels of training outcome. *Journal of Occupational and Organizational Psychology, 72*(3), 351–375. https://doi.org/10.1348/096317999166725

Warr, P., & Bunce, D. (1995). Trainee characteristics and the outcomes of open learning. *Personnel Psychology, 48*(2), 347–375. https://doi.org/10.1111/j.1744-6570.1995.tb01761.x

Wienrich, C., Reitelbach, C., & Carolus, A. (2021). The trustworthiness of voice assistants in the context of healthcare investigating the effect of perceived expertise on the trustworthiness of voice assistants, providers, data receivers, and automatic speech recognition. *Frontiers of Computer Science, 3*. https://doi.org/10.3389/fcomp.2021.685250

Wilder, D. A., Flood, W. A., & Stromsnes, W. (2001). The use of random extra credit quizzes to increase student attendance. *Journal of Instructional Psychology, 28*(2), 117–120.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *Proceedings of the international conference on information systems*. Paris, France.

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. (2012). Measuring mobile users'. *Concerns for information privacy 33rd international conference on information system*. Orlando: US.

Yi, J., Yuan, G., & Yoo, C. (2020). The effect of the perceived risk on the adoption of the sharing economy in the tourism industry: The case of Airbnb. *Information Processing & Management, 57*(1), Article 102108. https://doi.org/10.1016/j.ipm.2019.102108

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43*(3), 389–418. https://doi.org/10.1111/j.1745-6606.2009.01146.x

Zaman, S. R., Sadekeen, D., Alfaz, A., & Shahriyar, R. (2021). *One source to detect them all: Gender, age, and emotion detection from voice* 45th annual computers, software. *Applications conference (COMPSAC)*. Madrid, Spain.

Zarei, A. A. (2013). On the Learnability of three categories of Idioms by Iranian EFL learners. *Modares Educational Journal in TEFL, 2*(2), 82–100.

Zhong, B., & Yang, F. (2018). How we watch TV tomorrow?: Viewers' perception towards interactivity on smart TV. *International Journal of Asian Business and Information Management, 9*(4), 48–63. https://doi.org/10.4018/IJABIM.2018100104