Usability, Acceptance, and Trust of Privacy Protection Mechanisms and Identity Management in Social Virtual Reality

Jinghuai Lin*
HCI Group†
University of Würzburg

Christian Rack
HCI Group
University of Würzburg

Carolin Wienrich
PIIS Group‡
University of Würzburg

Marc Erich Latoschik
HCI Group
University of Würzburg

Figure 1: Our social VR prototype and the simulated exhibition social scenario. A) Users can put on the "Identity detector" goggles to find potential imposters. B) After putting on the goggles, avatars will be highlighted with visual effects indicating their identity status. C) Users can inspect each avatar's profile with the options to send a friend request, report (suspicious identities or activities) or ban the avatar from the virtual space.

Abstract

In social virtual reality (social VR), users are threatened by potential cybercrimes, such as identity theft, sensitive data breaches, and embodied harassment. These concerns are heightened by the increasing interest in the metaverse, the advancements in photorealistic 3D user reconstructions, and the rising incidents of online privacy violations. Designing secure social VR applications that protect users while enhancing their experience, acceptance and trust remains a challenge. This article investigates potential identity management solutions in social VR, and their impacts on usability and user acceptance. We developed a social VR prototype with novel and established countermeasures, including motion biometric verification, and conducted a study with 52 participants. Our findings reveal diverse preferences for identity management and underscore the importance of authenticity, autonomy, and reciprocity. Key findings include: passive verification is favored for pragmatic user experience, while active verification is preferred for its hedonic quality; continuous or periodic verification strengthens users' confidence in their privacy; and while user awareness promotes authentic engagement, it may also diminish the willingness to disclose personal information. This research not only offers foundational insights into the evaluated scenarios and countermeasures, but also sheds light on the designs of more trustworthy and inclusive social VR applications.

Index Terms: social virtual reality, metaverse, verification, authentication, privacy, identity, trust, usability, user study

1 Introduction

Social virtual reality (social VR), as a novel realm where interactions and experiences transcend physical boundaries, might be the very core aspect of the metaverse [13]. The advancements in immersive full-body interactions via avatars unlock the full potential of non-verbal communication compared to traditional social networks and communication tools. This enables socializing in shared virtual environments and provides tangible benefits for various applications (e.g., medical [48], educational [16], and work collaboration [14]), and creating an alternative realm for human sociocultural interaction [11]. As the boundaries between virtual reality (VR), augmented reality (AR), and mixed reality (MR) become increasingly blurred, the social features also extend beyond "immersive VR" to encompass extended reality (XR) [6].

However, the current state of social VR faces challenges in achieving widespread acceptance comparable to traditional social media: its applications are still primarily anchored in entertainment and socialization, with users often adopting alternative identities to engage in the virtual worlds [29, 12, 50]. The barriers could be manifold. Beyond the technological challenges, a key factor resides in the privacy concerns and identity risks users face in the convergence of virtual realities and social networks [38, 29]. For example, the risk of identity theft in social VR—where individuals replicate others' faces and identities, leading to social engineering attacks or privacy breaches—is on the rise, particularly with recent advancements in photorealistic 3D reconstruction of users [29]. The challenges also lie in ensuring the traceability and accountability of "citizens" in the virtual world, as various forms of cybercrime, including embodied harassment, have increasingly been reported [8, 47]. Furthermore, the sensitivity and breadth of user information collected and processed by XR devices and social VR applications [2] highlights the vulnerability and potential exploitation of personal data and user activities. On top of that, the inadequacy of corresponding ethical and regulatory frameworks further exacerbates such issues [2, 32].

Despite research and development efforts—including but not limited to motion biometric verification [19, 41], identity or trustworthiness indications [29], social privacy mechanisms [15, 35]—a significant gap remains in systematic usability evaluations and user-centered design guidelines for identity management (IDM) that encompass these countermeasures. To bridge the research gap, we implemented a social VR applications that incorporated both novel and existing countermeasures and IDM features (including user registration/login, motion-based verifications, avatar authenticity visualization, report/ban functions; more details in Section 3.3), and

*e-mail: jinghuai.lin@uni-wuerzburg.de
†Human-Computer Interaction Group
‡Psychology of Intelligent Interactive Systems Group

conducted a user study with 52 participants. Focusing on their influence on usability, user acceptance, and trust, the study assesses the effectiveness and usability of these protective measures, considering their psychological and sociological impacts and the emphasis on diverse user preferences. We identified and summarised key insights to provide user-centered design guidelines and offer a comprehensive strategy for enhancing security and trustworthiness in social VR environments.

2 Related work

2.1 Digital bodies and identity infringements

Typically, a social VR user controls a graphical self-representation of their choosing, commonly referred to as an avatar, to interact within the virtual environment and with each other. While avatars often adopt "fantasy" or stylized appearances [30], a personalized, photorealistic avatar that closely mirrors the user's real appearance [1] more effectively bridges their digital and real-world identities, enhancing the authenticity of social interactions in the virtual space [29, 49]. However, such "digital bodies" can inadvertently reveal users' real-life appearances and potentially their identities, which might not always be preferable due to privacy and security concerns. As there are limited measures to prevent a user from creating a digital body that replicates another's identity and likeness, such identity infringement could easily result in identity fraud and potentially have more significant consequences [29, 24]. Furthermore, digital bodies can easily be the targets of violent assault and sexual harassment [15]. Such assault and harassment could be far more intimate and emotionally harmful when the digital bodies represent one's true identity.

2.2 Motion-based biometric verification

User verification schemes (i.e., authentication), usually integrated with cryptographic protocols [18], are considered key components of an identity management system, confirming a user's identity or legitimacy [43]. Biometric methods [5] have the advantage of accuracy and security over traditional schemes (such as passwords) and are therefore widely applied in handheld devices and applications.

In the realm of XR devices and applications, common biometric modalities such as fingerprint and iris recognition have not yet been widely adopted due to both limited hardware availability and deployability. Nevertheless, given the significant volume of biometric information that XR devices collect and process, various XR modalities (e.g., body motions [41, 42, 37], eye movements [53], electroencephalogram (EEG) [26]) have been explored for novel biometric identification and verification [19], and show promising outcomes. Among these modalities, motion data inferred from HMD/controllers are versatile and provide stable identification performance across different consumer-grade devices [36], and have recently gained comprehensive research interest as the primary biometric modality for XR [19]. Notably, the recent work of Rack et al. [42] utilized a similarity-learning approach for motion verification, surpassing classification-learning in accuracy and readily adapting to new users without the need for comprehensive retraining.

These verification schemes can be further categorized into active and passive verification. Active verification necessitates that users perform one or more direct actions to complete the verification process; passive verification, in contrast, requires no conscious action on the part of the users [21], with the system verifying the users continuously [53] or periodically in the background. The frequency of user verification (e.g., one-time/static, continuous, periodic) is also highly relevant. While common schemes usually adopt one-time verification due to practicality, social VR sessions are considered long and continuously receive input through user interactions, thus coincide with continuous/periodic verification [54]. Previous studies on the usability of biometric verification have predominantly focused on modalities such as face recognition [20, 45, 23], fingerprint [45, 23], and keystroke traits [45], with an emphasis on the effects of continuous (passive) verification methods on cognitive load [20] or task completion [45, 23]. However, there is a notable gap in research on XR modalities (particularly motion biometrics), comparing the usability of active versus passive methods, or providing insights within the social VR privacy context. In addition to usability, we are interested in how verification attributes affect user trust and confidence in their privacy being protected. Therefore, in this study, we implemented both active and passive motion verification schemes with varying frequencies (one-time vs. continuous/periodic) and posed the following research question:

RQ1: How do motion verification attributes (especially passive vs. active and varying frequency) impact usability, user acceptance and trust in social VR applications?

2.3 User awareness and online disclosure

Research on traditional social media suggests that the willingness to share or disclose personal information is positively influenced by user awareness (the knowledge or ability of social networking tools and the understanding of privacy and security), trust, and privacy concerns [40]. Meanwhile, sharing consistent personal information across online and offline contexts enhances online authenticity and credibility [17], and helps establish alliance and trust[33]. Research has also indicated that self-disclosure patterns in social VR are akin to those in traditional social media [33].

However, social interactions within immersive VR environments still markedly differ from those on traditional social media, given the VR characteristics such as enhanced immersion, interactivity, and social presence. Furthermore, the unique challenges posed by photorealistic avatars and identity infringements have not yet been thoroughly addressed in this context. There is a lack of implementation of features or mechanisms that provide indications of identity and authenticity in social VR and empirical evidence of how the features are perceived and accepted.

Thus, one objective of our research is to delve deeper into the impact of user awareness and privacy concerns on identity and information disclosure, particularly in scenarios where users have access to protective mechanisms implemented in our application. This brought us to the following research questions:

RQ2: How do user awareness and privacy concerns change after accessing the protection mechanisms implemented in our system?

RQ3: How do the changes in awareness and privacy concerns influence users' acceptance of using their digital selves and real identities, and their personal information sharing in social VR?

Grasping user's self-disclosure patterns within the novel context of social VR, concerning privacy and identity issues, is crucial for understanding diverse user preferences and the development of user-centered protective measures.

2.4 Protection mechanisms and user preference

In addition to user verification, other countermeasures in social VR play a crucial role, as they not only protect users in practical terms but also empower them with control and autonomy over their actions in the virtual world. Additionally, understanding users' preferences regarding these countermeasures can offer valuable insights for further development and refinement. Falchuk et al. [15] presented design guidelines for privacy mechanisms in social VR that help protect users from several threats with a focus on harassment and observation. Most social VR applications also include the features to report, block other users [8], or to create a "space bubble" wherein other avatars vanish from the user's view if they get too close [35]. Lin et al. [28] investigated how visual identity indication influenced the perceived trustworthiness of avatars and provided design guidelines for signaling other users' authenticity sta-

tus. *VRChat* has also implemented a "trust rank" system [1] that assesses users' trustworthiness based on their time spent in *VRChat*, with nameplates color-coded to reflect this rank.

Such features and mechanisms translate abstract protections into visible and actionable options and align with user preferences, which is likely to enhance user trust. However, insights from user studies or design guidelines have previously focused on individual measures, leaving a gap in comprehensive research into the key factors of user-centered design for such protection mechanisms and exploration of users' diverse privacy preferences. Thus, the following research question could motivate the better design of future innovative protection mechanisms:

RQ4: What are the key factors in the design of protection mechanisms that enhance user acceptance and trust?

Despite efforts to enhance authenticity, the adoption of certain mechanisms might deter the engagement of users who prefer anonymity and potentially threaten user autonomy [27, 38]. For instance, in environments where most users are verified, those preferring to remain anonymous might feel discouraged from participating in social interactions. Similarly, implementing a "trust rank" system could compromise users' autonomy and their ability to independently judge whom to trust. Although most of the discussed countermeasures promote authenticity, comprehending the motivations behind anonymity and seeking protection for such preferences is essential. Currently implemented protections in social VR applications tend to prioritize authenticity, neglecting the alternative perspective. There is also a scarcity of relevant research on this issue. Therefore, we aim to investigate:

RQ5: How can users' autonomy and the choice for anonymity be safeguarded in social VR environments?

3 Method

To answer our research questions and contribute to design guidelines for social VR IDM development, we created a social VR application that features account registration/login, motion-based verification, avatar authenticity visualization, and report/ban functions, for participants to explore during a simulated experience. They interacted with various novel or existing identity management countermeasures, and provided feedback afterwards. This study has been approved by the institute's ethics committee. Our consent acquisition and data storage complied with local legislation and institutional requirements.

3.1 Design

To address RQ1, we implemented a 2 × 2 mixed design to examine the usability of different motion verification schemes and their impacts on user acceptance and trust (in both the system and other users). This involved "**passive**" and "**active**" verification as between-subject conditions, and the frequency of verification ("**always**" vs. "**once**") as a within-subject variable. The motion verification is based on the method of Rack et al. [42], utilizing a pre-trained similarity-learning model that verifies users with positional inputs of VR controllers, which requires no retraining and allows for real-time enrollment and verification. A novel "motion password" scheme was created as the "active" verification, requiring users to write a password with virtual hands (Figure 2A), intuitively combining task-driven and motion-based verification. Detailed technical descriptions and evaluations of the verification schemes are the subject of another ongoing work, and the algorithms/software will be openly available once published.

To address RQ2 and RQ3, our experiment used a within-subject design, assessing participants' willingness to 1) use their personalized photorealistic avatars and 2) true identity in different social VR scenarios (listed in Figure 4), and 3) share real personal information while using the application—**before** and **after** they experienced the all IDM features implemented.

For RQ4 and RQ5, we analyzed the effectiveness and user preference of each implemented protection mechanisms with descriptive results from customized rating scales and qualitative feedback via open questions in the post-experiment questionnaire.

3.2 Apparatus

The social VR application was implemented using Unity Engine[2] 2021.3.15f1 and ran on a VR-capable PC (Intel Core i9-13900K, Nvidia RTX 4070 Ti 12GB, 64GB RAM). The VR hardware consisted of an Oculus Quest 2 HMD and two controllers. The VR HMD was connected to the PC as PCVR through the Oculus Link service. In addition, pre- and post-questionnaires were implemented with LimeSurvey[3] 4.5.0. The application, questionnaires and other supplementary materials are publically available[4].

3.3 Procedure and Tasks

This subsection elaborates on the participants' tasks and activities within the VR experience, along with the underlying rationales and motivations for the designs.

Account registration. Participants first started by registering an account for the social VR application. The account registration phase included: 1) creating a username and password, 2) filling out the personal information (mandatory field: first and last name; optional field: gender, birthdate, location, email address, phone number), and 3) choosing an avatar (options were stylized low-poly or own photorealistic avatar [1]). Participants were clearly instructed to use the application as how they would in real life, with the discretion to provide real personal information or not. The account registration simulates a regular procedure of engaging an online social platform and reflects participants' willingness to share personal information and use personal photorealistic avatars.

Exploring a social scenario. Following registration, participants put on the VR headset, completed the basic interaction tutorial, and then entered an exhibition scene. They were not asked to complete certain tasks but were given audio instructions to explore the exhibition while being mindful of identity theft. Inside the virtual environment, there were 10 photorealistic avatars, some engaging in conversation and others observing the exhibits. It is worth noting that there are several "doppelgangers" in the scene—avatars with the same appearance and name —indicating the presence of identity theft. Pre-recorded audios were played automatically or triggered by experimenters as 'hints' to encourage participants to perform certain interaction (e.g., to put on the glasses and find out imposters). Participants were expected to: walk around the room and discover the "doppelgangers", put on the identity detector, inspect the profile of at least three avatars, and perform at least three times of banning/sending friend requests (which will require verification). The scenario helps participants to understand the potential novel threats to identity in social VR and emphasizes the importance of privacy protection and identity management.

Authenticity visualization. We introduce a novel "identity detector" goggles (Figure 1A) metaphor, which participants were encouraged to put on to help visualize avatars' authenticity and identify potential imposters (Figure 1B) in a dynamics "scanning" effect, following guidelines from the work of Lin et al[28]. They can also inspect each avatar's profile and "authenticity score", with the options to send a friend request, to report (suspicious identities or activities) or to ban the avatar (making it disappear from your virtual environment, similar to the "block" functions of several social VR applications (e.g., VRChat, Bigscreen)) (Figure 1C).

[1] https://docs.vrchat.com/docs/vrchat-safety-and-trust-system (accessed on 23/07/2024)

[2] https://unity.com/

[3] https://www.limesurvey.org/

[4] https://go.uniwue.de/idm-social-vr

Motion verification. Participants were required to be verified upon certain actions (e.g., sending friend requests, banning users), and were randomly divided into two groups with a 2 x 2 mixed design. In the active verification group, participants were required to use their "motion password" (writing the password in the air) for verification (Figure 2A). Conversely, the passive group was automatically verified through their motion, indicated by a circular progress bar (Figure 2B), and users were free to continue with other activities. For both groups, each participant tested the social VR prototype twice: in one session, verification was always required for certain actions (e.g., sending friend requests, banning users); in the other session, the verification only took place once. These sessions were on different days with the order counterbalanced, to minimize carryover effects. Following each session, participants provide real-time feedback (for details see Section 3.4) in VR within the same virtual environment. Notably, in the experiments the verification always returns a positive result, to avoid system failure and ensure comparability of participants' experience.

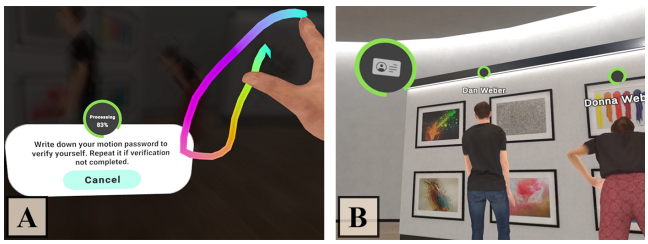

Figure 2: Two motion verification mechanisms: A) Active verification: the virtual environment fades into the dark with instructions to write down a password with virtual hands. The progress circle indicates the completion of the verification. B) Passive verification: users are automatically verified through their motion without conscious action. The progress circles appear at the top left corner of user's view and over the head of avatars that the user has performed actions to.

3.4 Measurements

Although the study was conducted in a controlled environment, the measurements were designed for participants to reflect alternative scenarios, individual preferences, and potential negative effects, rather than focusing solely on specific mechanisms. This approach allowed us to summarize design guidelines for social VR IDM from a broader, more general perspective.

Evaluation of motion verification. To evaluate the usability of the motion verification system, we adopted the short version User Experience Questionnaire (UEQ-S) [46] for its simplicity and applicability as real-time feedback in VR. The Technology Acceptance Model [34] was not adopted, due to its construct and items especially those under the Perceived Usefulness category not fitting well with the social context or the purpose of IDM. Alternatively, the Trust of Automated System Test (TOAST) [52] was chosen to assess users' trust and acceptance of verification functionalities and reliability. Six custom Likert-scale questions (see Table 1) were included for feedback on user acceptance, impacts on self-disclosure, and confidence in their privacy. In addition, qualitative feedbacks of the presented verification system were collected through an open question in the post-questionnaire.

Digital bodies, identity and information disclosure. Participants' willingness to use personalized photorealistic avatars and true identities in different scenarios was measured on 1-to-7 Likert scales both in the pre- and post-questionnaires. In the post-questionnaire, we asked participants to indicate the real personal information (i.e., first name, last name, birthdate, location, email address, phone number) they provided during the account registration and the information they would provide after the experiment as a descriptive behavioral measure of personal information sharing.

Privacy preference on other protection mechanisms. During the VR experience, only one visual indication ("scanning effect") was presented. In the post-questionnaire, we showcased alternative visualizations [28] to ensure a comprehensive understanding of the purpose of the visualization system and asked for quantitative feedback through customized Likert scales (***VQ1:*** *I found the visual indications help me to evaluate other users' identity easily;* ***VQ2:*** *I would trust avatars with positive indicators (e.g., the green outline) more compared to avatars with negative indicators (e.g., the red outline);* ***VQ3:*** *In a social VR application, I wish these visual indications are always visible (such visual indication can simply be an icon floating above the avatar's head);* ***VQ4:*** *In a social VR application, I wish these visual indications are only visible when I active them (e.g., put on a "Identity detector", or activate them through setting menu)*) and qualitative feedback to descriptively assess effectiveness and user preferences.

We also proposed an alternative way to display all the detailed information that determines an avatar's authenticity in addition to the "overall score" (see Figure 1C) in the application. Participants rated how much they like the two designs in 7-point Likert scale and provide quantitative feedback on their Preference.

Lastly, participants were presented with four options for identity visibility (***Option 1:*** *Each user has an authenticity status, and is visible to every user;* ***Option 2:*** *Users can choose whether to disclose their identity status to others or not. If they choose not to, other users will find that their authenticity status is not visible;* ***Option 3:*** *Similar to option 2, users can choose whether to disclose their identity status to others or not. However, if they turn off their authenticity status, they won't be able to check other users' status as well;* ***Option 4:*** *All users' Authenticity status is not visible by default. Users can give permission to each other to see their status (similar to a friend list)*). Participants rated how much they like the four options in 7-point Likert scale and provide quantitative feedback on their Preference.

The questionnaires also collect participants' demographics, familiarity with VR and social VR, and established tests such as simulation sickness [7].

4 Results

52 participants (10 males and 42 females) with an average age of 21.69 (SD = 2.32) recruited via the university participant recruitment system completed the experiment. 84.62% of them have experienced virtual reality at least one time before, and 5.77% have experienced virtual reality more than 50 times; 53.85% of them have used social VR applications at least one time before, but only 1.92% have used them more than 10 times.

4.1 Evaluation motion verification

The motion verification mechanisms were evaluated using UEQ-S, TOAST, and custom questions (items listed in Table 1) with a mixed design. Two-way mixed ANOVA, or robust mixed ANOVA [31] when the normality or variance homogeneity assumptions were not met, were performed. Descriptive results are presented Table 1.

4.1.1 UEQ-S

Results of UEQ-S (-3 to +3 Likert scales) were computed into a **total** score, and two subscales: **pragmatic quality** score, and **hedonic quality** score [46]. For the total score, no significant main effect of Group (active vs. passive) ($F(1, 50) = 0.46$, $p = 0.503$) or Frequency (once vs. always) ($F(1, 50) = 0.02$, $p = 0.889$), nor interaction ($F(1, 50) = 0.35$, $p = 0.559$) was found.

For the **pragmatic quality** score, the robust mixed-ANOVA with 20% trimmed means revealed a significant main effect of Group (active vs. passive), $F(1, 29.66) = 4.20$, $p = 0.0495$; participants

Table 1: Descriptive results of UEQ-S, TOAST, and custom questions on different motion verification mechanisms. Between: "passive" vs "active" verification; within: frequency "always" vs. "once".

		active × once	active × always	passive × once	passive × always
	Range	*M(SD)*	*M(SD)*	*M(SD)*	*M(SD)*
UEQ-S					
Pragmatic quality	[-3 – 3]	0.76 (0.61)	0.53 (0.77)	0.97 (0.82)	0.77 (0.78)
Hedonic quality	[-3 – 3]	1.18 (0.83)	1.29 (0.73)	0.65 (1.33)	0.93 (0.85)
Total	[-3 – 3]	0.97 (0.54)	0.91 (0.43)	0.81 (0.85)	0.85 (0.72)
TOAST					
Understanding	[1 – 7]	5.41 (0.91)	5.60 (0.84)	5.08 (0.82)	5.13 (0.81)
Performance	[1 – 7]	5.02 (1.01)	5.45 (1.10)	5.32 (0.81)	5.45 (0.87)
Total	[1 – 7]	5.19 (0.79)	5.52 (0.74)	5.21 (0.64)	5.31 (0.67)
Custom questions					
(CQ1) I would like to use this kind of authentication method (Motion Password) in social VR. (*authentication current*)	[1 – 7]	4.85 (1.32)	5.15 (1.43)	5.00 (1.41)	5.27 (1.31)
(CQ2) In general, I would like to be authenticated in social VR. (*authentication general*)	[1 – 7]	5.27 (1.64)	5.50 (1.50)	5.00 (1.77)	5.27 (1.64)
(CQ3) In general, I would like to use my personalized photorealistic avatar in social VR. (*digital body*)	[1 – 7]	3.81 (1.63)	3.96 (1.48)	3.85 (1.69)	4.39 (1.63)
(CQ4) In general, I would use my real identity in social VR (similar to people use their real identity on social media such as Facebook). (*real identity*)	[1 – 7]	3.77 (1.63)	4.04 (1.71)	4.15 (1.74)	4.39 (1.58)
(CQ5) I believe that my identity and privacy are safe on this social VR platform. (*privacy confidence current*)	[1 – 7]	3.77 (1.37)	4.04 (1.56)	3.92 (1.52)	4.00 (1.47)
(CQ6) In general, I believe that my identity and privacy are safe on social VR platforms. (*privacy confidnce general*)	[1 – 7]	3.39 (1.33)	3.62 (1.58)	2.81 (1.20)	3.23 (1.37)

considered the passive verification (M = 1.02, SD = 0.75) better completing the task or reaching the goals than the active verification (M = 0.69, SD = 0.68) (Figure 3A). No main effect of Frequency (F (1, 29.76) = 3.02, p = 0.093) nor interaction (F (1, 29.76) = 0.004, p = 0.95) was found.

For the **hedonic quality** score, there was a marginally significant main effect of Group (active vs. passive), F (1, 50) = 3.43, p = 0.070, η^2 = 0.052; participants had more pleasure or fun whiling using the active verification (M = 1.24, SD = 0.78) than the passive verification (M = 0.79, SD = 1.11) (Figure 3B). No main effect of Frequency (F (1, 50) = 2.59, p = 0.114, η^2 = 0.010) nor interaction (F (1, 50) = 0.52, p = 0.473, η^2 = 0.002) was found.

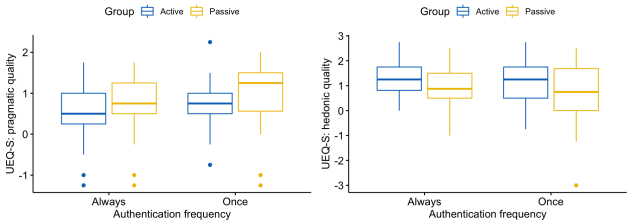

Figure 3: Box plots for the subscales of UEQ-S. A) UEQ-S pragmatic quality score; B) UEQ-S hedonic quality score.

4.1.2 TOAST

Results of TOAST (1 to 7 Likert scales) were computed into a **total** score, and two subscales: **understanding** score, and **performance** score [52]. For the **total** score, there was a significant main effect of frequency (always vs. once), F (1, 50) = 4.28, p = 0.044, η_2 = 0.023; the overall trust is significantly higher in the condition "always" (M = 5.41, SD = 0.71) than in the condition "once" (M = 5.20, SD = 0.71). No main effect of Group (F (1, 50) = 0.272, p = 0.604, η^2 = 0.004) nor interaction (F (1, 50) = 1.24, p = 0.271, η^2 = 0.007) was found.

For the **understanding** score, the robust mixed-ANOVA found no significant main effect of Group (F (1, 29.37) = 0.2.34, p = 0.137) or Frequency (F (1, 28.17) = 0.005, p = 0.945), nor interaction (F (1, 28.17) = 0.84, p = 0.368).

For the **performance** score, the robust mixed-ANOVA with 10% trimmed means revealed a significant main effect of frequency, F (1, 40.40) = 4.75, p = 0.035; it indicates that participants felt significantly more confident in the system performance in the condition "always" (M = 5.52, SD = 0.92) than in the condition "once" (M = 5.21, SD = 0.98). No main effect of Group (F (1, 40.83) = 0.214, p = 0.646 nor interaction (F (1, 40.60) = 1.14, p = 0.291) was found.

4.1.3 Custom questions

For custom question 3 (**CQ3**), there was a significant main effect of Frequency (always vs. once), F(1, 50) = 5.04, p = 0.029, η_2 = 0.012; the condition "always" (M = 4.17, SD = 1.56) was rated significantly higher than the condition "once" (M = 3.83, SD = 1.64), indicating that participants were more willing to use their personalized photo-realistic avatars in social VR under higher verification frequency condition. No main effect of Group (F (1, 50) = 0.30, p = 0.58, η^2 = 0.005) nor interaction (F (1, 50) = 1.56, p = 0.218, η^2 = 0.004) was found.

For **CQ6**, the robust mixed-ANOVA with 10% trimmed means revealed a significant main effect of Frequency (always vs. once), F(1, 37.60) = 5.95, p = 0.0196; the condition "always" (M = 3.38, SD = 1.57) was rated significantly higher than the condition "once" (M = 3.07, SD = 1.54), indicating that participants considered social VR platforms safer under higher verification frequency condition. No main effect of Group (F (1, 41.20) = 1.62, p = 0.211) nor interaction (F (1, 37.60) = 0.49, p = 0.490) was found. There was no main effect or interaction for other CQs.

On an average level, participants were fond of using motion verification (**CQ1**) (M = 5.07, SD = 1.36) and being authenticated in social VR in general (**CQ2**) (M = 5.30, SD = 1.58). The willingness to use their personalized photorealistic avatars (**CQ3**) (M = 4.00, SD = 1.60) and real identity (**CQ4**) (M = 4.09, SD = 1.66)

were at medium levels. The ratings for considering their identities and privacy safe on the presented social VR platform (**CQ5**) (M = 3.93, SD = 1.46) were significantly higher than that on social VR platforms in general (**CQ6**) (M = 3.26, SD = 1.39), with mean of the differences 0.67, t (103) = 6.1844, p <0.001, d = 0.606.

4.1.4 Qualitative feedback

Qualitative feedback was collected after the first session. Three participants (P20, P26, P34) who experienced the active verification complained that repeating the verification process was "annoying" and "cumbersome". Conversely, no participants from the Group "passive" had similar complaints. P37 mentioned that it is good to be able to "continue working during the verification process" in the passive verification. Four participants (P5, P19, P39, P44) expressed security concerns about the process; P19 was concerned about how much personal information can be unintentionally learned by others through motion biometrics. P5 would like to have more information on the data storage and verification process when using such a system.

4.2 Digital bodies, identity and information disclosure

We evaluated participants' willingness to use personalized photorealistic avatars and real-life identities through 1-to-7 Likert scales in pre- and post-questionnaires. We also compared whether users would share authentic personal information before and after trying out the prototype. The following results (Section 4.2 and 4.3) were considered independent from the manipulation of verification methods, as they investigated different concepts and tests from various aspects detected no significant influence.

Willingness to use personalized photorealistic avatars. Due to the violation of the normality assumption, a Friedman test was performed at the scenario level both before and after participants tried out the prototype: the willingness to use photorealistic avatars significantly differed in different scenarios both before (χ_2 (8) = 40.70, p <0.001, W = 0.10) and after (χ_2 (8) = 48.50, p <0.001, W = 0.12) the experiment (Figure 4A). Wilcoxon Signed-Rank tests at the time (before vs. after) level revealed a significant increase from before to after the experiment in the Business scenario (p = 0.034, r = 0.25[5]), and marginally significant increases in Financial (p = 0.096, r = 0.19) and Entertainment scenarios (p = 0.062, r = 0.20). Different in other scenarios are non-significant.

Willingness to use real-life identity. Due to the violation of the normality assumption, a Friedman test was performed at the scenario level both before and after the tryout: the willingness to use real-life identity significantly differed in different scenarios both before (χ_2 (8) = 197, p <0.001, W = 0.47) and after (χ_2 (8) = 162, p <0.001, W = 0.39) the experiment. (Figure 4B). Wilcoxon Signed-Rank test at the time (before vs. after) level revealed significant increases from before to after the experiment in the Game (p = 0.046, r = 0.21) and Entertainment scenarios (p = 0.044, r = 0.28), and a marginally significant increase in the General scenario (p = 0.077, r = 0.28). Different in other scenarios are non-significant.

Personal information sharing. Figure 4C illustrates the percentage of real information participants were willing to provide in user profiles before and after the experiment. McNemar's tests showed a significant decrease in the sharing of real "last name" (p <0.001) and "location" (p = 0.016) information. Differences in other items are non-significant.

4.3 Privacy preference on other protection mechanisms

We evaluated participants' preferences for various IDM user interface designs and collected qualitative feedback. All responses were measured on 1-to-7 Likert scales.

[5]Wilcoxon effect size [39]

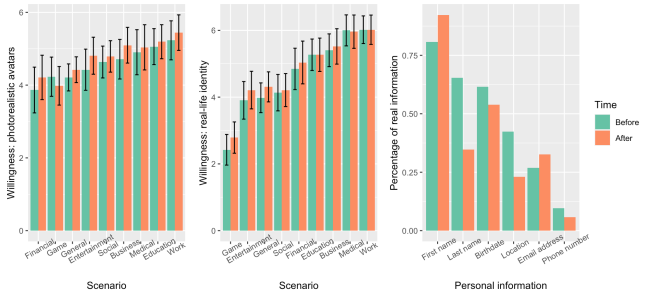

Figure 4: A) Willingness to use personalized photorealistic avatars in different social VR scenarios, before and after the experiment; B) willingness to use real-life identity in different social VR scenarios, before and after the experiment; A) the percentages of participants providing real personal information, before and after the experiment.

4.3.1 Visual identity indicators.

Participants generally found visual indicators (VIs) on avatars useful for easy identity evaluation (**VQ1**) (M = 6.31, SD = 1.18) and would be likely to trust avatars with positive indicators more compared to those with negative indicators (**VQ2**) (M = 6.48, SD = 0.96). A Wilcoxon signed-rank test showed no significant preference for visual identity indicators being always visible (**VQ3**) (M = 5.02, SD = 1.66) versus only being visible when activated by themselves (**VQ4**) (M = 4.39, SD = 2.22), p = 0.191.

Qualitative feedback. The qualitative feedback revealed a more profound divergence compared to the ratings of **VQ3** and **VQ4**. Most participants explicitly favored either the "constantly visible" option (N = 25) or the "visible by activation" option (N = 22). Among those preferring the VIs to be always visible, many (N = 9) mentioned it helps in immediately recognizing the authenticity of others at first glance; three participants felt that constantly-visible VIs offered a sense of "security" and "transparency". Conversely, among those who favored VIs being visible only upon activation, many (N = 5) found a constantly-visible VI to be "annoying", "disrupting", and "distracting"; some voiced concerns that permanent VIs could "make the avatars unrealistic", deter the "naturalness of the environment" or "weakening the perception of reality"; several (N = 5) felt that constant-visible VIs could lead to biased impressions, making them "conditioned in advance how I evaluate a person" (P47). Additionally, five participants noted that their choice depended on the context and scenario. For example, in contexts like gaming, the identity and consequent display of VIs were deemed less relevant. A few suggestions included only permanently displaying VIs for "dangerous" or "suspicious" avatars (N = 3), or having the VIs appear by default at the initial contact with an unknown avatar (P13).

4.3.2 Authenticity score

There was no significant preference difference between seeing others' "authenticity status" as detailed information (M = 5.23, SD = 1.76) or as an overall score (M = 5.10, SD = 1.51), p = 0.92, according to a Wilcoxon signed-rank test.

Qualitative feedback. In the qualitative feedback, while the predominant advantage noted for the overall score was that it is "easy" or "user-friendly" and helps to have a quick overview (N = 14). Conversely, the main benefits of detailed information were that it helps to understand better what contributes to the authenticity (N = 10), or it is more "transparent" (N = 2) and "authentic" (N = 2).

While many (N = 9) recommended to have both the options displayed, the primary concern against detailed information was the reluctance to share such information (N = 5), and felt "more compelled to give the site more data" (P19). On the other hand, many (N

= 9) valued autonomy, preferring to assess situations or authenticity independently by themselves, rather than "those that the system finds good or not" (P21). P40 suggested that overall scores would be more user-friendly but emphasized the necessity of sufficient research into the factors influencing these scores.

4.3.3 Identity visibility options

A Friedman test revealed significant differences in the scoring of different privacy options (see Section 3.4), χ^2 (3) = 31.90, p <0.001, W = 0.20. Pairwise Wilcoxon signed-rank tests indicated significant differences between **Option 1** (M = 5.21, SD = 1.75) and **Option 2** (M = 3.33, SD = 2.06), p <0.001, r = 0.53; **Option 2** and **Option 3** (M = 5.58, SD = 1.51), p <0.001, r = 0.74; and **Option 3** and **Option 4** (M = 4.21, SD = 2.00), p = 0.002, r = 0.50.

Qualitative feedback. The preference ranking (Option 3 >Option 1 >Option 4 >Option 2) were well reflected in qualitative feedback. **Option 2** faced the most criticism, primarily for creating an "unfair" situation (N = 4) for authenticated users. **Option 1** was appreciated for its transparency (N = 4), enhanced security (N = 2) and making it "easier to trust the system" (P17). However, it was also considered an invasion of privacy by some (N = 2), and many (N = 7) preferred to have control over the disclosure of their authenticity. Three participants considered **Option 1** as more suitable for more "serious" or "professional" contexts (e.g., business, medical). **Option 4** was favored for pure social space (P7) and for allowing user to grant permission only to trusted individuals (N = 3). Criticisms included that it potentially hinders interaction, "as the start of the interaction is subject to a further preliminary step and in some cases, this is perceived as stressful or not natural" (P1), and "annoying if you constantly have to share permissions" (P12). There are also concerns about excessive anonymity (P34) and uncertainty (P47). For **Option 3**, many (N = 9) valued its fairness and reciprocity, and some (N = 5) liked that it provides a middle ground between privacy (anonymity) and security (authenticity).

When it came to the main criteria or concerns influencing their decisions: many (N = 11) viewed fairness and reciprocity as crucial. Some (N = 4) were primarily concerned with the freedom of anonymity or disclosure: "...when it comes to a private setting... the disclosed status feels like a "social credit" system. It feels like a surveillance tool that is at odds with freedom and individualization" (P20). Conversely, many (N = 8) showed explicit favor for more authenticity: "I think that if you don't want to reveal your identity, it always looks like you have something to hide and I want to be able to interact with real people in such a VR world" (P41); "I think it's good if there is some kind of tool in the virtual world to identify people and that no identity theft can take place"(P49). Two participants mentioned that the feature to ban avatars with low authenticity makes them feel safe and secure. Last but not least, many (N = 7) emphasized autonomy, valuing the ability to choose what information to reveal and to whom, "It is important to decide for yourself what information you want to reveal, but there should be no pressure to reveal your own information about yourself" (P1).

5 Discussions

To address our research questions (RQs), we summarize our main findings and the implications for the future development of social VR in the following aspects.

5.1 Evaluation of motion verification

Our findings offer several intriguing insights for **RQ1** and the design of social VR verification systems. While feedback was based on the assessed methods, participants were not informed nor required to understand the specific implementation details (such as which modalities were used for verification). Therefore, observations drawn from usability and user experience can to some extent generalize to social VR biometric verification with different techniques: (1) Passive verification was perceived to have a higher pragmatic quality (i.e., they describe interaction qualities that relate to the tasks or goals the user aims to reach when using the product [46]), active verification scored higher in hedonic quality (i.e., they do not relate to tasks and goals, but describe aspects related to pleasure or fun while using the product [46]), and they contributed to a similar level of usability. Combined with qualitative feedback, this could imply that passive verification offers a smoother, less disruptive user experience, while active verification heightens user engagement and possibly also introduces elements of fun and novelty, particularly for first-time users. (2) Meanwhile, the frequency of verification influenced users' trust in the system. Continuous or periodic verification, while potentially necessary for improved security, also appears to strengthen users' confidence in their privacy. However, if combined with active verification, it could also lead to feelings of annoyance and frustration.

Although further investigation is necessary, the above findings could still hold for different verification modalities (e.g., eye movement) and therefore provide shared insights. For instance, to harness the strengths of both approaches, at the point of logging into applications, users could undergo active verification through direct interaction. This step not only grants them a sense of control but also heightens their awareness of the security process. Subsequently, passive verification can occur, designed not to interrupt their ongoing activities. Given that users report increased confidence in their privacy through continuous or periodic checks, implementing discreet yet reassuring signals during passive verification can enhance their sense of security without being intrusive.

5.2 Identity and information disclosure

After experiencing our social VR system with its proposed and tested IDM features, participants showed greater willingness to use their real identity or a personalized photorealistic avatar in several scenarios. Interestingly, the willingness to use real identity showed large variability across scenarios and a distinct ranking trend.

Overall, there is low interest in sharing personal information on social VR platforms, with the exception of first names (which might significantly depends on cultural factors, as in some cultures the isonymy of first name is uncommon). Although most people considered identity authenticity important and were keen on being authenticated, many preferred to disclose less information after participating in our social VR evaluation. This finding aligns with Paramarta et al.[40], indicating that user awareness negatively impacts personal information sharing, yet contradicts findings by Benson et al. [4], that user awareness and security notices have a positive effect on information disclosure.

Moreover, the increasing willingness among users to adopt personalized photorealistic avatars (in contexts like business, finance, and entertainment) or their real-life identities (in gaming and entertainment) sends an encouraging signal. It suggests that, at least in certain scenarios the protection mechanisms can motivate users to present their true selves within the virtual world. Although our participants have limited prior exposure to social VR and thus unlikely to have experienced all the scenarios, their responses, influenced by their prior experiences with traditional social media, provide insights into the attitudes of a broader demographic of potential social VR users. This aids in understanding how new users may engage in various social VR scenarios and how their acceptance of such technology may be influenced.

These findings provide some valuable insights to answer **RQ2** and **RQ3**: (1) users' awareness, including their proficiency in using social media sites and their understanding of privacy and security, positively influences their acceptance of entering the virtual world as themselves, though the impact varies depending on the context. (2) Users desire greater authenticity in social VR, both from oth-

ers and themselves, but this doesn't necessarily translate to sharing extensive personal information. (3) IDM systems that assist in increasing overall authenticity and therefore enhancing trust should be achieved without compelling users to compromise their privacy.

Such trends also align closely with the current landscape of social VR platforms and their user base. In popular communities (e.g., *VRChat*, *RecRoom*, and *Bigscreen*), it's rare for users to reveal their real identities, whether by choosing photorealistic avatars that resemble them or displaying their real names. Conversely, despite a reluctance to disclose real identities, there exists a strong demand for improved safety and trust mechanisms to facilitate genuine interactions.

5.3 Privacy preference on other protection mechanisms

In line with the findings of Lin et al. [28], participants were generally pleased with the visual identity indicators, which helped them assess the authenticity and trustworthiness of others. While some believed that a constant indication would maintain transparency and offer a sense of security within the social VR community, many felt that it could disrupt interactions or reduce the plausibility of the virtual world, echoing prior findings [28]. It could be inferred from qualitative feedback that context matters; for instance, in contexts such as finance where authenticity is emphasized, users would prefer to receive constant feedback. In more casual or social situations, the preference is to leave the choice to the users.

The preference for the system's authenticity feedback is beyond a matter of usability; it also pertains to users' concerns about privacy and autonomy. Although a one-dimensional overall score might be more user-friendly, users were more concerned that it could create bias and influence users' autonomy. Given the extent to which user autonomy is already manipulated on traditional social media [44], these concerns are not unfounded. As a similar example, the "trust rank" system implemented by *VRChat*, though intended to signify a user's "trustworthiness," has faced significant criticism: this one-dimensional ranking, based purely on time spent on the platform, can sometimes be misleading. It may even incentivize users to engage in unnecessary online activities to achieve a higher rank, rather than genuinely contributing to the community's well-being. Therefore, future research or development needs to delve deeper into the determinants of online authenticity and how to objectively reflect them, while ensuring that users are able to make autonomous judgments to a greater extent.

The preference for identity visibility indicates diverse views on authenticity and anonymity. Participants particularly value mechanisms like *Option 3* that enables users control over identity disclosure and offers reciprocity, thus fostering a positive cycle of overall authenticity of the community. Meanwhile, we must not overlook the needs of those who prefer anonymity. Whether such mechanisms could segregate users and hinder their active participation in virtual community activities requires further contemplation and exploration.

While these findings do not fully resolve **RQ4** and **RQ5**, they allow us to pinpoint several critical factors consistently highlighted during the evaluation of the proposed mechanisms. These include a preference for authentic interactions, the importance of fairness and reciprocity in information sharing, the value of anonymity, and the autonomy to make trust-based decisions. Consideration of such factors will not only benefit the deployment of existing mechanisms but also the future design of novel solutions.

5.4 Limitations

Firstly, the demographic skew in our sample, particularly the limited age range and occupational diversity, may restrict the generalizability of our findings. Secondly, the experiment was conducted in a simulated setting without real social interactions, which might not fully capture the complexities and dynamics of actual usage scenarios. Last but not least, although the questionnaires yielded valuable qualitative feedback, it could be enhanced by employing more interactive methods like semi-structured interviews or workshops to gain more detailed and comprehensive insights.

5.5 Future work

In our study, we evaluated a social VR prototype enriched with various protection mechanisms. Building on this work's insights and guidelines, future research could explore and compare additional mechanisms, as well as assess their impact in specific settings like workplaces or educational environments.

To increase generalizability and gain more real-world insights, future studies could integrate protection mechanisms into commercial platforms and conduct studies with actual social VR users and adequate exposure time. Including a broader demographic range would allow for detailed subgroup analyses to investigate the impact of demographic factors. Meanwhile, implicit action and behavioral data (e.g., route path within the virtual environment [51], eye gaze [22], velocity of action [25], physiological signal [9]) can be recorded and analyzed as objective measures and enhance the results derived from subjective measures [10].

Given the user preference for metrics like "authenticity score" or "trust rank" in facilitating social decision-making, conducting in-depth research on this topic is imperative. A thorough understanding and identification of the determinants of online authenticity are essential.

6 Conclusion

This work presented a social VR applications that incorporated with IDM and privacy protection features, and conducted user evaluations to assess their usability and impact on user acceptance and trust. Our findings reveal that passive verification is associated with higher pragmatic quality, enhancing user experience by aligning closely with their tasks and goals. Active verification, on the other hand, is perceived to offer greater hedonic quality, enriching the user experience with elements of pleasure and engagement. Additionally, we found that the implementation of continuous or periodic verification methods bolsters users' confidence in the protection of their privacy.

Our findings also show the positive influence of users' awareness on their propensity to engage authentically within the virtual environment. However, this increased awareness paradoxically discourages the sharing of personal information, suggesting a nuanced relationship between user awareness and privacy behaviors in social VR. Participants expressed varied preferences for protection mechanisms, underscoring a collective valuation of authenticity, autonomy, and reciprocity. These preferences highlight the critical role of user-centered design in developing social VR platforms that prioritize user trust and engagement.

As a first step towards establishing design guidelines for identity management in social VR, our study aims to inspire further research and development. We envision our work help to create secure, reliable, and inclusive social VR platforms, enabling practical applications for socio-cultural interaction and seamlessly extending real-life activities.

Acknowledgments

This work is part of the Privacy Matters (PriMa) project. The PriMa project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 860315. This work was also supported by the Bavarian State Ministry for Digital Affairs in the project XR Hub (Grant A5-3822-2-16). Special thanks to Yousof Shehada, Felix Achter, and Lukas Schach for their help in development and conducting the experiments.

REFERENCES

[1] J. Achenbach, T. Waltemate, M. E. Latoschik, and M. Botsch. Fast generation of realistic virtual humans. In *Proceedings of the 23rd ACM Symposium on Virtual Reality Software and Technology*, VRST '17, pp. 1–10. Association for Computing Machinery, New York, NY, USA, 2017. doi: 10.1145/3139131.3139154 2, 3

[2] D. Adams, A. Bah, C. Barwulor, N. Musaby, K. Pitkin, and E. M. Redmiles. Ethics emerging: the story of privacy and security perceptions in virtual reality. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pp. 427–442, 2018. 1

[3] S. Banaeian Far and S. M. Hosseini Bamakan. NFT-based identity management in metaverses: challenges and opportunities. *SN Applied Sciences*, 5(10):260, Sept. 2023. doi: 10.1007/s42452-023-05487-5

[4] V. Benson, G. Saridakis, and H. Tennakoon. Information disclosure of social media users: Does control over personal information, user awareness and security notices matter? *Information Technology & People*, 28(3):426–441, Jan. 2015. Publisher: Emerald Group Publishing Limited. doi: 10.1108/ITP-10-2014-0232 7

[5] D. Bhattacharyya and R. Ranjan. Biometric Authentication: A Review. *Science and Technology*, 2(3), 2009. 2

[6] M. Billinghurst, P. Cesar, M. Gonzalez-Franco, K. Isbister, J. Williamson, and A. Kitson. Social XR: The Future of Communication and Collaboration (Dagstuhl Seminar 23482). *Dagstuhl Reports*, 13(11):167–196, 2024. doi: 10.4230/DagRep.13.11.167 1

[7] P. Bimberg, T. Weissker, and A. Kulik. On the Usage of the Simulator Sickness Questionnaire for Virtual Reality Research. In *2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pp. 464–467. IEEE, Atlanta, GA, USA, Mar. 2020. doi: 10.1109/VRW50115.2020.00098 4

[8] L. Blackwell, N. Ellison, N. Elliott-Deflo, and R. Schwartz. Harassment in Social Virtual Reality: Challenges for Platform Governance. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):100:1–100:25, 2019. doi: 10.1145/3359202 1, 2

[9] T. T. Brunyé and G. E. Giles. Methods for eliciting and measuring behavioral and physiological consequences of stress and uncertainty in virtual reality. *Frontiers in Virtual Reality*, 4, Jan. 2023. Publisher: Frontiers. doi: 10.3389/frvir.2023.951435 8

[10] C. de Juan-Ripoll, J. Llanes-Jurado, I. A. C. Giglioli, J. Marín-Morales, and M. Alcañiz. An Immersive Virtual Reality Game for Predicting Risk Taking through the Use of Implicit Measures. *Applied Sciences*, 11(2):825, Jan. 2021. Number: 2 Publisher: Multidisciplinary Digital Publishing Institute. doi: 10.3390/app11020825 8

[11] J. D. N. Dionisio, W. G. B. Iii, and R. Gilbert. 3D Virtual worlds and the metaverse: Current status and future possibilities. *ACM Computing Surveys*, 45(3):1–38, June 2013. doi: 10.1145/2480741.2480751 1

[12] J. Dong, M. Dong, and K. Ota. Exploring Avatar Experiences in Social VR: A Comprehensive Analysis of User Reviews. *IEEE Consumer Electronics Magazine*, 2024. Publisher: IEEE. 1

[13] Y. K. Dwivedi, L. Hughes, A. M. Baabdullah, S. Ribeiro-Navarrete, M. Giannakis, M. M. Al-Debei, D. Dennehy, B. Metri, D. Buhalis, C. M. K. Cheung, K. Conboy, R. Doyle, R. Dubey, V. Dutot, R. Felix, D. P. Goyal, A. Gustafsson, C. Hinsch, I. Jebabli, M. Janssen, Y.-G. Kim, J. Kim, S. Koos, D. Kreps, N. Kshetri, V. Kumar, K.-B. Ooi, S. Papagiannidis, I. O. Pappas, A. Polyviou, S.-M. Park, N. Pandey, M. M. Queiroz, R. Raman, P. A. Rauschnabel, A. Shirish, M. Sigala, K. Spanaki, G. Wei-Han Tan, M. K. Tiwari, G. Viglia, and S. F. Wamba. Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 66:102542, Oct. 2022. doi: 10.1016/j.ijinfomgt.2022.102542 1

[14] R. Evard, E. F. Churchill, and S. Bly. Waterfall Glen: Social Virtual Reality at Work. In E. F. Churchill, D. N. Snowdon, and A. J. Munro, eds., *Collaborative Virtual Environments: Digital Places and Spaces for Interaction*, Computer Supported Cooperative Work, pp. 265–281. Springer, London, 2001. doi: 10.1007/978-1-4471-0685-2_14 1

[15] B. Falchuk, S. Loeb, and R. Neff. The Social Metaverse: Battle for Privacy. *IEEE Technology and Society Magazine*, 37(2):52–61, June 2018. Conference Name: IEEE Technology and Society Magazine. doi: 10.1109/MTS.2018.2826060 1, 2

[16] K. Foerster, R. Hein, S. Grafe, M. E. Latoschik, and C. Wienrich. Fostering Intercultural Competencies in Initial Teacher Education. Implementation of Educational Design Prototypes using a Social VR Environment. In *Innovate Learning Summit*, pp. 95–108. Association for the Advancement of Computing in Education (AACE), 2021. 1

[17] O. L. Haimson, T. Liu, B. Z. Zhang, and S. Corvite. The Online Authenticity Paradox: What Being "Authentic" on Social Media Means, and Barriers to Achieving It. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):423:1–423:18, 2021. doi: 10.1145/3479567 2

[18] Y. Huang, Y. J. Li, and Z. Cai. Security and Privacy in Metaverse: A Comprehensive Survey. *Big Data Mining and Analytics*, 6(2):234–247, June 2023. Conference Name: Big Data Mining and Analytics. doi: 10.26599/BDMA.2022.9020047 2

[19] J. M. Jones, R. Duezguen, P. Mayer, M. Volkamer, and S. Das. A Literature Review on Virtual Reality Authentication. In S. Furnell and N. Clarke, eds., *Human Aspects of Information Security and Assurance*, IFIP Advances in Information and Communication Technology, pp. 189–198. Springer International Publishing, Cham, 2021. doi: 10.1007/978-3-030-81111-2_16 1, 2

[20] D. M. Kaburu, J. Sansa-Otim, K. Mayanja, D. P. Mirembe, and T. Bulega. A usability based approach to designing continuous user biometric authentication system. *Quality and User Experience*, 3(1):8, June 2018. doi: 10.1007/s41233-018-0021-1 2

[21] Y. Kakizaki, R. Doine, K. Kuwana, and M. Yoshida. Implementing passive authentication with enhanced risk-based security. In *2022 16th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, pp. 78–83, Oct. 2022. doi: 10.1109/SITIS57111.2022.00020 2

[22] J. L. Kröger, O. H.-M. Lutz, and F. Müller. What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking. In M. Friedewald, M. Önen, E. Lievens, S. Krenn, and S. Fricker, eds., *Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers*, pp. 226–241. Springer International Publishing, Cham, 2020. doi: 10.1007/978-3-030-42504-3_15 8

[23] G. Kwang, R. H. C. Yap, T. Sim, and R. Ramnath. An Usability Study of Continuous Biometrics Authentication. In M. Tistarelli and M. S. Nixon, eds., *Advances in Biometrics*, pp. 828–837. Springer, Berlin, Heidelberg, 2009. doi: 10.1007/978-3-642-01793-3_84 2

[24] J. Lake. Hey, You Stole My Avatar!: Virtual Reality and Its Risks to Identity Protection. *EMORY LAW JOURNAL*, 69:48, 2020. 2

[25] H. Lee, H. Kim, D. V. Monteiro, Y. Goh, D. Han, H.-N. Liang, H. S. Yang, and J. Jung. Annotation vs. Virtual Tutor: Comparative Analysis on the Effectiveness of Visual Instructions in Immersive Virtual Reality. In *2019 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*, pp. 318–327, Oct. 2019. ISSN: 1554-7868. doi: 10.1109/ISMAR.2019.00030 8

[26] S. Li, S. Savaliya, L. Marino, A. M. Leider, and C. C. Tappert. Brain Signal Authentication for Human-Computer Interaction in Virtual Reality. In *2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, pp. 115–120, Aug. 2019. doi: 10.1109/CSE/EUC.2019.00031 2

[27] J. Lin. Can Social VR Substitute Real Life? From a Perspective of Identity, Privacy, and Authenticity, Nov. 2022. 3

[28] J. Lin, J. Cronjé, C. Wienrich, P. Pauli, and M. E. Latoschik. Visual Indicators Representing Avatars' Authenticity in Social Virtual Reality and Their Impacts on Perceived Trustworthiness. *IEEE Transactions on Visualization and Computer Graphics*, 29(11):4589–4599, Nov. 2023. doi: 10.1109/TVCG.2023.3320234 2, 3, 4, 8

[29] J. Lin and M. E. Latoschik. Digital body, identity and privacy in social virtual reality: A systematic review. *Frontiers in Virtual Reality*, 3, 2022. 1, 2

[30] Q. Liu and A. Steed. Social Virtual Reality Platform Comparison and Evaluation Using a Guided Group Walkthrough Method. *Frontiers in Virtual Reality*, 2:668181, May 2021. doi: 10.3389/frvir.2021.668181

2

[31] P. Mair and R. Wilcox. Robust Statistical Methods Using WRS2. 4

[32] D. Maloney, G. Freeman, and A. Robb. Social Virtual Reality: Ethical Considerations and Future Directions for An Emerging Research Space. *arXiv:2104.05030 [cs]*, Apr. 2021. arXiv: 2104.05030. 1

[33] D. Maloney, S. Zamanifard, and G. Freeman. Anonymity vs. Familiarity: Self-Disclosure and Privacy in Social Virtual Reality. In *26th ACM Symposium on Virtual Reality Software and Technology*, pp. 1–9. ACM, Virtual Event Canada, Nov. 2020. doi: 10.1145/3385956.3418967 2

[34] N. Marangunić and A. Granić. Technology acceptance model: a literature review from 1986 to 2013. *Universal Access in the Information Society*, 14(1):81–95, Mar. 2015. doi: 10.1007/s10209-014-0348-1 4

[35] c. McCarthy. The "space bubble" ensures you always have personal space in VR, July 2016. 1, 2

[36] R. Miller, N. K. Banerjee, and S. Banerjee. Within-System and Cross-System Behavior-Based Biometric Authentication in Virtual Reality. In *2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pp. 311–316. IEEE, Atlanta, GA, USA, Mar. 2020. doi: 10.1109/VRW50115.2020.00070 2

[37] V. Nair, C. Rack, W. Guo, R. Wang, S. Li, B. Huang, A. Cull, J. F. O'Brien, M. Latoschik, L. Rosenberg, and D. Song. Inferring Private Personal Attributes of Virtual Reality Users from Head and Hand Motion Data, June 2023. arXiv:2305.19198 [cs]. doi: 10.48550/arXiv.2305.19198 2

[38] F. O'Brolcháin, T. Jacquemard, D. Monaghan, N. O'Connor, P. Novitzky, and B. Gordijn. The Convergence of Virtual Reality and Social Networks: Threats to Privacy and Autonomy. *Science and Engineering Ethics*, 22(1):1–29, Feb. 2016. doi: 10.1007/s11948-014-9621-1 1, 3

[39] J. Pallant. *SPSS Survival Manual: A step by step guide to data analysis using IBM SPSS*. Routledge, London, 7 ed., July 2020. doi: 10.4324/9781003117452 6

[40] V. Paramarta, M. Jihad, A. Dharma, I. C. Hapsari, P. I. Sandhyaduhita, and A. N. Hidayanto. Impact of User Awareness, Trust, and Privacy Concerns on Sharing Personal Information on Social Media: Facebook, Twitter, and Instagram. In *2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*, pp. 271–276. IEEE, Yogyakarta, Oct. 2018. doi: 10.1109/ICACSIS.2018.8618220 2, 7

[41] C. Rack, A. Hotho, and M. E. Latoschik. Comparison of Data Encodings and Machine Learning Architectures for User Identification on Arbitrary Motion Sequences. In *2022 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR)*, pp. 11–19, Dec. 2022. ISSN: 2771-7453. doi: 10.1109/AIVR56993.2022.00010 1, 2

[42] C. Rack, K. Kobs, T. Fernando, A. Hotho, and M. E. Latoschik. Versatile User Identification in Extended Reality using Pretrained Similarity-Learning, Apr. 2024. arXiv:2302.07517 [cs]. doi: 10.48550/arXiv.2302.07517 2, 3

[43] J. Ryu, S. Son, J. Lee, Y. Park, and Y. Park. Design of Secure Mutual Authentication Scheme for Metaverse Environments Using Blockchain. *IEEE Access*, 10:98944–98958, 2022. Conference Name: IEEE Access. doi: 10.1109/ACCESS.2022.3206457 2

[44] S. Sahebi and P. Formosa. Social Media and its Negative Impacts on Autonomy. *Philosophy & Technology*, 35(3):70, July 2022. doi: 10.1007/s13347-022-00567-7 8

[45] E. Schiavone, A. Ceccarelli, A. Bondavalli, and A. M. Carvalho. Usability Assessment in a Multi-Biometric Continuous Authentication System. In *2016 Seventh Latin-American Symposium on Dependable Computing (LADC)*, pp. 43–50, Oct. 2016. doi: 10.1109/LADC.2016.17 2

[46] M. Schrepp, A. Hinderks, and J. Thomaschewski. Design and Evaluation of a Short Version of the User Experience Questionnaire (UEQ-S). *International Journal of Interactive Multimedia and Artificial Intelligence*, 4(6):103, 2017. doi: 10.9781/ijimai.2017.09.001 4, 7

[47] K. Schulenberg, G. Freeman, L. Li, and C. Barwulor. "Creepy Towards My Avatar Body, Creepy Towards My Body": How Women Experience and Manage Harassment Risks in Social Virtual Reality. *Proceedings of the ACM on Human-Computer Interaction*, 7(CSCW2):236:1–236:29, 2023. doi: 10.1145/3610027 1

[48] D. Shao and I.-J. Lee. Acceptance and Influencing Factors of Social Virtual Reality in the Urban Elderly. *Sustainability*, 12(22):9345, Jan. 2020. Number: 22 Publisher: Multidisciplinary Digital Publishing Institute. doi: 10.3390/su12229345 1

[49] L. Stacchio, M. Perlino, U. Vagnoni, F. Sasso, C. Scorolli, and G. Marfia. Who will Trust my Digital Twin? Maybe a Clerk in a Brick and Mortar Fashion Shop. In *2022 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pp. 814–815, Mar. 2022. doi: 10.1109/VRW55335.2022.00258 2

[50] K. Thoidou and V. Zorbas. VR and Social Identity The utilisation of Virtual Reality Technology for the study of Social Identity in children with a migrant background situated in Greece. 2022. 1

[51] P. Tian, Y. Wang, Y. Lu, Y. Zhang, X. Wang, and Y. Wang. Behavior Analysis of Indoor Escape Route-Finding Based on Head-Mounted VR and Eye Tracking. In *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 422–427, July 2019. doi: 10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00090 8

[52] H. Wojton, D. Porter, S. Lane, C. Bieber, and P. Madhavan. Initial validation of the trust of automated systems test (TOAST). *The Journal of Social Psychology*, 160:1–16, Apr. 2020. doi: 10.1080/00224545.2020.1749020 4, 5

[53] Y. Zhang, W. Hu, W. Xu, C. T. Chou, and J. Hu. Continuous Authentication Using Eye Movement Response of Implicit Visual Stimuli. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 1(4):177:1–177:22, 2018. doi: 10.1145/3161410 2

[54] H. Zhong, C. Huang, X. Zhang, and M. Pan. Metaverse CAN: Embracing Continuous, Active, and Non-Intrusive Biometric Authentication. *IEEE Network*, 37(6):67–73, Nov. 2023. doi: 10.1109/MNET.2023.3318890 2