Mine Yourself!: A Role-playing Privacy Tutorial in Virtual Reality Environment

Junsu Lim*
Daegu Gyeongbuk Institute of Science and Technology
Daegu, Republic of Korea
junsu@dgist.ac.kr

Hyeonggeun Yun*
Agency for Defense Development
Daejeon, Republic of Korea
yhg8423@gmail.com

Auejin Ham*
Korea Advanced Institute of Science and Technology
Daejeon, Republic of Korea
hamaj@kaist.ac.kr

Sunjun Kim
Daegu Gyeongbuk Institute of Science and Technology
Daegu, Republic of Korea
sunjun_kim@dgist.ac.kr

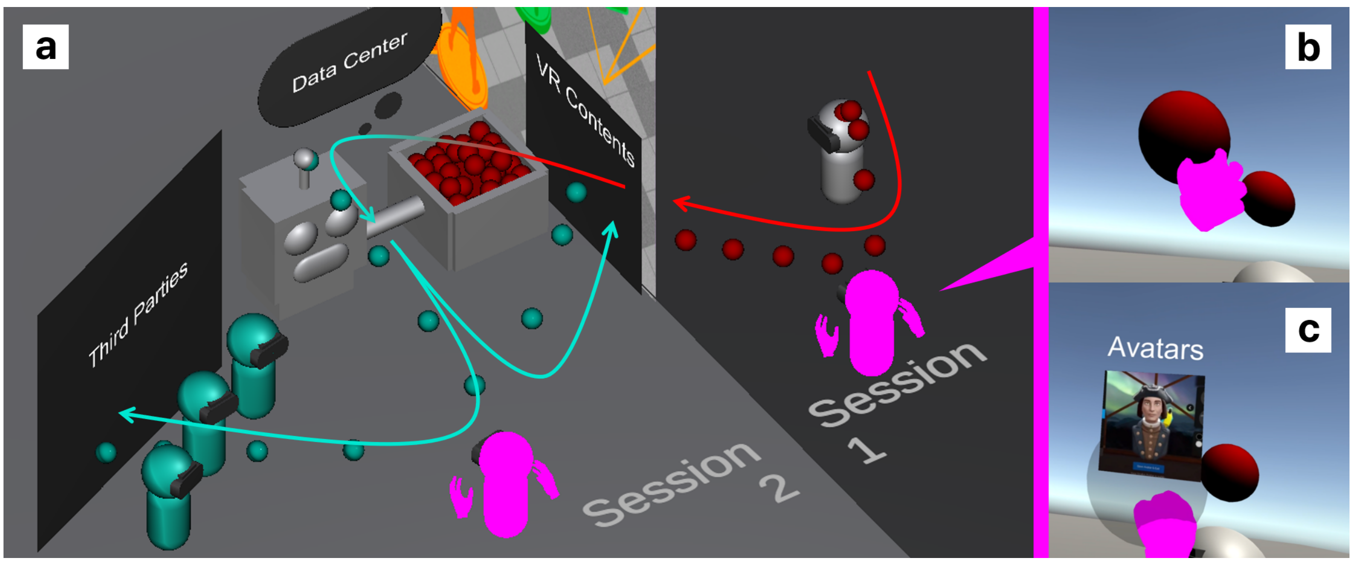


Figure 1: Our VR privacy tutorial consists of two role-playing sessions: data collection (*Session 1*), and data utilization and distribution (*Session 2*). Users, colored in magenta, (a) serve as data channels between VR devices, VR contents, and third parties. Users are asked to (b) catch balls with VR data inside, (c) check the data by name and example image, and throw those to designated destinations.

ABSTRACT

Virtual Reality (VR) has potential vulnerabilities in privacy risks from collecting a wide range of data with higher density. Various designs to provide information on Privacy Policy (PP) have improved the awareness and motivation towards privacy risks. However, most of them have focused on desktop environments, not utilizing the full potential of VR's immersive interactivity. Therefore, we proposed a role-playing mechanism to provide an immersive experience of interacting with PP's key entities. First, our formative study found insights for PP where VR users had limited awareness of what data to be collected and how to control them. Following this, we implemented a VR privacy tutorial based on our role-playing mechanism and PP from off-the-shelf VR devices. Our privacy tutorial increased a similar amount of privacy awareness with significantly higher satisfaction (p=0.007) than conventional PP. Our tutorial also showed marginally higher usability (p=0.11).

*These authors contributed equally to this research.

CHI '22 Extended Abstracts, April 29-May 5, 2022, New Orleans, LA, USA

ACM ISBN 978-1-4503-9156-6/22/04.
https://doi.org/10.1145/3491101.3519773

CCS CONCEPTS

• **Security and privacy** → **Usability in security and privacy**; • **Human-centered computing** → **Empirical studies in HCI**; **Virtual reality**; **Visualization systems and tools**.

KEYWORDS

virtual reality, privacy, role-playing, privacy policy, privacy tutorial

ACM Reference Format:
Junsu Lim, Hyeonggeun Yun, Auejin Ham, and Sunjun Kim. 2022. Mine Yourself!: A Role-playing Privacy Tutorial in Virtual Reality Environment. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '22 Extended Abstracts), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3491101.3519773

1 INTRODUCTION

Privacy concerns are emerging in Virtual Reality (VR). VR packed with dense sensors, VR gears are capable of collecting a vast amount of information than before [1, 25]. Not only traditional text and image data generated from users, but VR could also further collect infringe personal biometric data (e.g., eye gaze, body movement, size of a hand, breathing pattern, and brain wave signal) [1, 16, 21, 34]. Those biometric data are invariable, unlike passwords or credit card numbers, hence risker. Also, biometric information could allow inferring of users' thoughts and feelings [1, 11], which is further threatening human rights. Unlike non-VR environments, additional personal information could be extracted by combining biometric data and user's environment data in the VR environment [10]. For example, Meta (former Facebook), who is operating a VR platform named Oculus series, is notoriety collecting user information and was recently fined $650 million for violating Illinois' biometric law (BIPA) by collecting biometric data without the user's consent [31].

Privacy Policy (PP) supposes to inform users about the details of collected data; most of them have poor user experiences (UX) from extensive use of jargon [15, 26]. Therefore, most users do not read them and press a consent button [4, 15] while unawarely providing personal information. Users struggle to demand compensation with database leakage accidents, contrary to GDPR article 82 [46] because they agreed to a PP they have not read. As we mentioned, PP in VR has more potential risks than regular services, while PP presented in VR is far less readable, which may escalate the problem [20]. We addressed this problem by gamifying PP in a role-playing game instead of presenting PP as-is inside VR. We expect gamification to increase users' understanding of their privacy problems and provide better UX in general.

In the following, we present a formative study consists of a semi-structured interview and a drawing session to get users' awareness about using VR devices. A role-playing privacy tutorial was designed and implemented based on the corpus and diagrams obtained from the qualitative feedback of the formative study. Finally, we conducted a preliminary user study for empirical validation to check whether the privacy tutorial would be able to improve the user's awareness against the original PP in VR.

2 BACKGROUND AND RELATED WORK

We briefly review the prior works related to visualizing Terms of Service and Privacy Policy, security and privacy issues on VR, and the role-playing method's efficacy.

2.1 Visualizing Policy

'Notice and choice' are two cores of the privacy policy [47]. 'Notice' is a policy presentation (e.g., Terms of Service, Privacy Policy), and 'choice' is users' agreement on the presented policy. Policy documents mostly consist of jargon and long sentences; therefore, alternative visualization of policy has been tried [17, 38, 45]. Visualizing policy gains more user attractiveness, stimulation, and novelty, and more policy viewing time [38]. PPs presented in VR have the same problem, and the existing visualization solutions are less effective because of the many confounding factors such as location, angle, and depth of elements around the user, as well as poor readability within VR environment [20]. As a new alternative design, we propose a role-play-based solution that could increase usability by interacting with elements directly rather than a passive reading experience.

2.2 Security and Privacy Risks of VR

VR devices possibly threaten user privacy further than other personal gears. They could collect richer high-fidelity information, like always-on external cameras, motion sensors, and even biometric sensors [16, 35, 39, 42]. Those biometric data such as eye movement and breathing patterns might be used to infer additional information such as health information and interest of users [10]. For instance, [42] showed that eye movement could be used to infer gender, age, and users' interest in a scene. Furthermore, breathing pattern of users could be utilized to provide feedback in a VR exercising game [21].

Crimes in a data-rich VR environment could be even more severe than other crimes on a traditional personal computer. VR is more resembling real-world and possibly induces deeper emotions in users [18, 33, 48], as well as physical harms [50]. Also, passing sensitive personal information to third-party [25], which are often included in PP agreements, could further threaten users [35].

2.3 Efficacy of Role-playing Method

Role-playing is used in the psychotherapy, education and entertainment [5, 9, 19, 29, 32]. The user is immersed in the role as the user thinks and acts according to the given environment when they play the role [29]. In psychological therapy, it has been shown that this immersion can improve subjects' emotional awareness [22]. Such role-playing in specific situations can positively or negatively impact users [5, 29].

In this research, we compare a gamified role-playing privacy tutorial of PP against regular text-based PP. We expect the gamified PP to improve poor user experience and better understand privacy threats lurking inside PP.

3 FORMATIVE STUDY

Before developing a role-playing privacy tutorial, we first needed to understand users' awareness of privacy concerns on VR. We extracted users' mental models about VR privacy to find key potential factors and supplemented them through the tutorial introduced in the following section. A formative study was conducted with nine participants (age M=22.33, SD=2.00, five males and four females) recruited from a local university. Four participants were never experienced VR (inexperienced users) and five participants had VR experience at least once (experienced users).

3.1 Formative Study Design and Procedure

We designed a two-session study to obtain a mental model of users' general ideas and privacy concerns on VR. A session consisted of a semi-structured interview and drawing exercise on a presented topic. We designed the semi-structured interview following Huang et al.'s approach [14]. All sessions were audio-recorded to analyze qualitative data. One session took an hour on average.

In the first session, we asked *"Could you describe your understanding of how the VR device works?"*. They drew their understanding of how the VR device works (see the mental model drawing example part of supplementary materials for details). Then, the participants described their drawings and highlighted the critical points. After the drawing session, we interviewed to understand participants' general idea of VR. We asked questions about the usage of VR devices, knowledge of VR devices, where to use VR devices, and general concerns with VR devices.

In the second session, we asked *"Could you describe your understanding of privacy concerns in the VR device?"*, and a similar procedure to the first session proceeded. In the interview, we asked about features of VR devices that bother participants, access to third parties, data protection towards VR devices, data collection through VR devices, data control, and reasons to trust or not to trust companies. We also asked experienced users questions about their experience on reading Privacy Policy (PP). To prevent bias on participants' privacy concerns, we did not ask about privacy issues that participants did not mention during the interview. See the formative study guide part of supplementary materials for details of the formative study design.

3.2 Formative Study Result

We analyzed the corpus extracted from the interviews and drawings based on qualitative content analysis [28] to find the codes and the relations among them. We used open coding to find the primary thoughts of each participant in the study. After that, we used axial coding to combine participants' thoughts and find general insights on VR privacy concerns.

We found four major topics and analyzed them in the formative study (see the table of formative study analysis results part of supplementary materials for details).

(1) We analyzed participants' common knowledge of VR privacy problems. Most participants were able to mention personal data collected by VR content providers and companies. However, all they mentioned were common data, which could be also collected by an ordinary mobile devices. No participants mentioned VR-specific data such as body tracking, interaction, and 3D surrounding environments for collision prevention [1]. Some participants mentioned that cyberattacks might occur towards VR.

(2) We analyzed their common thoughts over VR privacy problems. We found that most participants were not aware of or did not concern about VR privacy problems and potential privacy issues. Interestingly, even though some participants mentioned discomfort towards collecting personal information, most of them said they felt no control over what data to collect. We found out that several participants had a passive attitude towards privacy problems.

(3) We analyzed the user perception on content providers and companies. We found that participants had naive understanding of collected data protection. They trusted VR content providers and companies. Moreover, most participants said that third parties were not accessible to their personal data except for a particular case.

(4) We analyzed the usability problems in Privacy Policy (PP) in VR. We found that every participant did not read and understand current PP despite the importance of privacy and data collection problems. Most participants mentioned they did not feel the current PP was valuable and helpful. This led us to design interactive tutorials for immersive in VR to supplement the original PP.

We concluded that participants had insufficient knowledge and motivation to take action about potential privacy risks in VR, and conventional PP in VR is limited to aid this problem. These findings align with what existing literature [10, 13] have proposed implying that conventional PPs of other digital media are difficult to mitigate risks in VR due to its immerse nature. Based on our findings, we derived three main insights for our implementation to (1) increase users' privacy awareness about data collection and utilization in VR, (2) provoke motivations for self-defense towards VR privacy issues, and (3) provide an immersive environment for the more comfortable understanding of PP.

4 IMPLEMENTATION

4.1 Role-playing Tutorial

From the formative study, we found that awareness of what data is collected and how to control its range is the critical issue of PP. Also, people struggled to understand how their private data spreads within a system. Our design follows the idea of visualizing policy for better awareness [17, 38, 45], and further leveraging full modalities of the VR environment by adopting role-playing methods. Role-playing allows participants to experience different perspectives [29, 44] and encourages critical thinking and creativity [5]. Also, physically embodied designs offer affordances for aiding in the meaning-making process [30, 36, 37]. Therefore, we expect the role-playing method to provide a more 'interactive' way of understanding what data might be collected while using VR, achieving better understanding and awareness of privacy concerns in VR.

4.2 Tutorial Design

The role-playing scene consists of a user avatar, VR contents, data center, content providers, and third parties (see Figure 1) as entities. Participants serve as a medium to transfer privacy data between the components during tutorial sessions. Each privacy data is abstracted as a ball (*data ball*); participants can hold or toss it using their controllers. We defined a list of privacy data (*keywords*), tutorial sessions, and entities based on Oculus Privacy Policy [25].

We divided our VR privacy tutorial into two sessions: one for data collection; and the other for the utilization and distribution of collected data (see Figure 2). Each session requires participants to deliver data balls consecutively from one entity to another. Each data ball has a randomly assigned keyword, determining the destination entity. Participants are instructed to (1) grab each data ball, (2) read data keyword inside it, and (3) throw it into the designated entity or discard it by dropping it to the ground. When all keywords are successfully collected, the session finishes.

We selected keywords for both sessions from Oculus PP: Session 1 (Physical Features, Avatars, Voice Interactions, Environmental Data, Movement Data, and Info from Third Parties), and Session 2 (XR Features, Avatars, Social Features, Voice Interactions, and In-app Activity). We also presented each data keyword as an image to

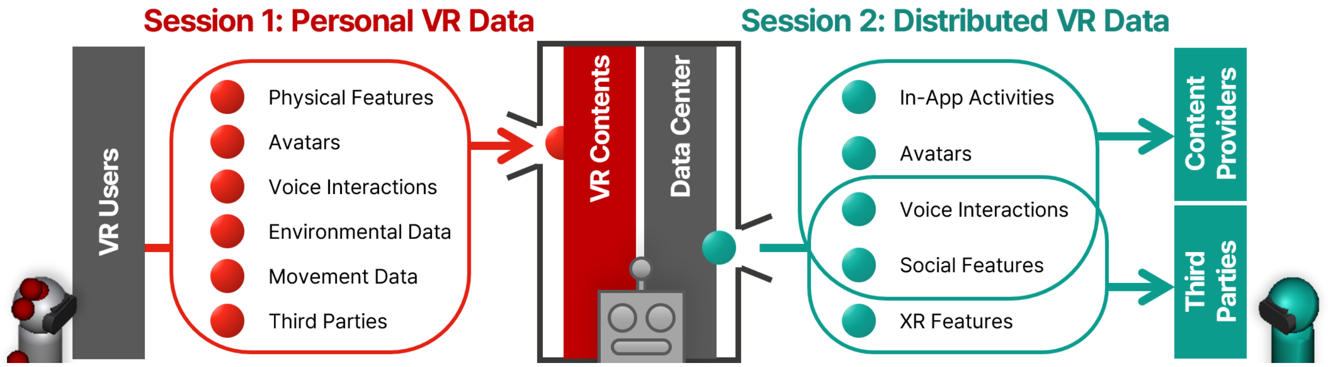


Figure 2: Overview of the transmission of personal data during our privacy tutorial. Private data from VR users are collected into VR content. After then, those data are utilized by the data center and distributed to content providers and third parties.

invoke awareness in privacy data [12]. A virtual narrator provided verbal instructions (using Kakao Speech API [8]) in a controlled manner.

4.2.1 Session 1: Data Collection. In this session, the participants observe what data is collected from VR users. They are guided to throw data balls generated from 'VR users' inside the hit range of 'VR contents.' Participants must throw data balls containing the keyword three times consecutively for each of the six data keywords used in this session. One of the two balls has the wrong keyword, forcing participants to check keywords each time they grab it. Therefore, in this session, participants are expected to read keywords 36 times (i.e., six keywords × three consecutive balls to throw × two expected times to check each keyword). Participants can learn different types of data collected by VR content, visual examples of those data, and our tutorial's role-playing metaphor through this session.

4.2.2 Session 2: Data Utilization and Distribution. In the second session, two destination entities (i.e., content providers and third parties) receive data balls from the data center. Since data balls are assigned to one destination, participants are forced to keep in mind (1) what data keyword to throw and (2) where to throw. Figure 2 shows what keywords we used for the two entities; we defined seven tasks as pairs of keyword and destination entity. Therefore, participants are expected to read keywords 42 times (i.e., seven tasks × three consecutive balls to throw × two expected times to check each keyword). Through this session, participants can learn different types of private data that might be utilized and distributed by VR content providers, visual examples of those data, and their destination.

5 PRIVACY TUTORIAL USER STUDY

We conducted a preliminary user study to evaluate the efficacy of the privacy tutorial. We recruited fourteen participants (age M=24.14, SD=1.46, 12 males and 2 females, native Korean speakers) from a local university. They were paid USD $10 equivalent for the participation. The University Internal Review Board (IRB) approval was obtained.

5.1 Experiment Condition

The study used a between-subjects design with two conditions: Privacy Policy (PP) and Privacy Tutorial (PT). In the PP condition, participants read a PDF file containing Oculus's PP downloaded the Oculus Data Policy website [25] on a 13-inch monitor for 10 minutes. The PP contents were written in Korean and presented in 12pt font. Participants were able to rescale the size of the PDF file if they were necessary. To match with PT condition, we highlighted eleven keywords (e.g., Physical Features, Avatars, Voice Interactions, Environmental Data, Movement Data, Info from Third Parties, XR Features, Avatars, Social Features, Voice Interactions, and In-app Activity) used in the PT condition. In PT condition, participants wore Oculus Quest and played our privacy tutorial system implemented with Unity engine. The participants played the two sessions (data collection and data utilization & distribution – check Section 4.2 for the details).

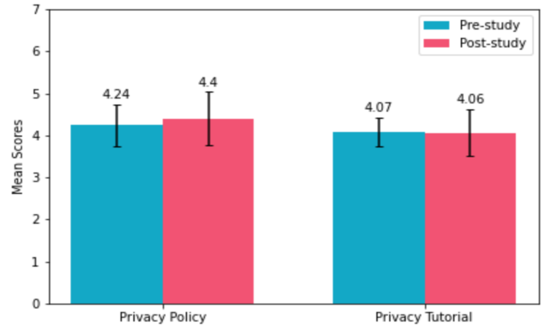
5.2 Measurement

We performed qualitative and quantitative analysis. For qualitative analysis, participants drew and explained their mental models about VR privacy problems before and after the study, similar to the formative study. For quantitative analysis, participants answered questionnaires about privacy awareness before and after the experiment, and they answered another set of questionnaires (usability, satisfaction, and burden) after the experiment. The questionnaires were designed based on existing literature [2, 6, 7, 23, 24, 27, 40, 43, 49], and a 7-point Likert scale (1 as *strongly disagree*, and 7 as *strongly agree*) was used (see supplementary materials for details). We used Wilcoxon Signed Rank Test to compare privacy awareness scores between pre and post-study. We used Mann Whitney U Test to compare the scores between the conditions for other questionnaires.

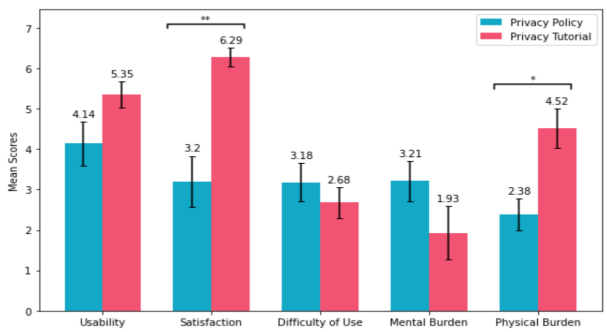
5.3 Procedure

After welcoming participants, we introduced the general information and process of the study. After the participants understood the process and agreed with the study, we randomly assigned either PP or PT conditions.

Pre-study Session. Before the main study, we asked a question *"Could you describe your understanding of privacy concerns in the VR*



(a)



(b)

Figure 3: (a): Mean score of participants' privacy awareness before experiment and after experiment, (b): Usability, satisfaction, difficulty of use, and burdens in Privacy Policy and Privacy Tutorial, *: p < 0.05, **: p < 0.01

device?" and participants drew and explained their mental models about VR privacy concerns based on the question. After the drawing session, they answered 7-point Likert scale questionnaires about privacy awareness.

Main-study Session. Each participant performed the main experiment with their assigned condition (PP or PT). PT condition cost around 10 minutes on average, with some variance depending on the different skills of participants. We also assigned 10 minutes for PP condition to read the Privacy Policy document displayed on the screen.

Post-study Session. After the main experiment, the participants drew and explained their mental models about VR privacy concerns. Subsequently, they answered another 7-point Likert scale questionnaires about their privacy awareness and their experiment condition's quantitative measures (usability, satisfaction, and burden).

5.4 Results

5.4.1 Quantitative Results. Before getting into the main analysis, we calculated Cronbach's alpha (α) for each set of questionnaires. Since $\alpha > 0.60$, we concluded that the questionnaires were answered consistently and were valid for the statistical analysis.

First, we analyzed privacy awareness (α = 0.93) scores between pre and post-study with Wilcoxon Signed Rank Test (see Figure 3a). In the PP condition, the privacy awareness of post-study was higher than that of pre-study, but there was no significant difference ($V = 7, p = 0.52$). In the PT condition, the privacy awareness of post-study and the privacy awareness of pre-study was no significant difference ($V = 13, p = 0.94$). As a result, there were no significant differences in the privacy awareness between pre and post-study in both PP and PT.

Second, we compared usability (α = 0.88) and satisfaction (α = 0.92) of PP and PT with Mann Whitney U Test (see Figure 3b). In usability, the PT condition was higher than the PP condition, but there was no (or marginal) significant difference ($W = 37.5, p = 0.11$). In satisfaction, the PT condition was significantly higher than PP condition ($W = 46, p = 0.007$). Although there was no significant difference in usability, the satisfaction in PT is higher than in PP. A positive effect could not be confirmed in usability, but a positive effect could be confirmed in satisfaction.

Finally, we compared the burden of PP and PT with the Mann Whitney U Test (see Figure 3b). The burden consisted of difficulty of use (α = 0.67), mental burden (α = 0.90), and physical burden (α = 0.93). In the difficulty of use, the PT condition was lower than the PP condition, but there was no significant difference ($W = 17.5, p = 0.40$). In mental burden, the PT condition was lower than the PP condition, but there was no significant difference in the two conditions ($W = 12.5, p = 0.12$). In physical burden, the PP condition was significantly lower than PT condition ($W = 44, p = 0.01$). This means that PT is more physically demanding than PP.

5.4.2 Qualitative Results. We analyzed interview corpus, and mental model results of participants through qualitative content analysis [28]. Subsequently, we found differences in participants' mental models before and after the study.

Personal Thoughts about VR. In the pre-study session, some participants (N=3 in PT, N=1 in PP) did not think about personal information and data leakage. P1 (PT) said, "I did not think personal information would be exposed." Furthermore, many participants (N=3 in PT and N=4 in PP) did not know what was happening with VR. For instance, P10 (PP) said, "I do not know what will happen if I use VR devices." In the post-study session, some participants mentioned that restrictions against VR were not established as those in real life (N=2 in PP). P12 (PP) said, "I do not think sanctions in VR have been established as much as those applied in real life."

Collection and Usage of Data towards VR. In the pre-study session, a few participants (N=1 in PT, N=3 in PP) mentioned that VR device collects personal information such as voice, video, and motion data without consent. Also, a few participants said that VR companies use data for customized advertisement (N=2 in PT, N=3 in PP). P9 (PP) mentioned, "VR is more advantageous to do personalized advertisements than PC because it could collect the whole set of movements and tastes." Some participants thought there were no privacy problems towards VR (N=1 in PT, N=3 in PP) and that the personal data was not meaningful. P6 (PT) said, "I think it is meaningless to collect individual activities or access records." However, in the post-study session, participants' perspectives differed from the pre-study interview. First, many participants (N=5 in PT, N=7 in PP) recognized that VR device collects personal information such as voice, video, and motion data without consent. For example, P6 (PT) said, "I think VR companies collect much information at once." Also, they mentioned that VR companies use data for customized advertisements. Some participants (N=2 in PT, N=3 in PP) were concerned about the abuse of data and centralized data management of VR companies. P10 (PP) said, "I think it is bad for companies to control information from VR devices."

Access of Third Parties. In the pre-study session, all participants did not mention the usage of data and information towards third parties. However, in the post-study session, many participants (N=5 in PT, N=4 in PP) understood third parties' access to data. They said that personal information could be provided to third parties or VR contents provider. P9 (PP) said, "It comes to mind that information can be shared with a considerable number of third parties." Few participants (N=1 in PT, N=1 in PP) were concerned about third parties' data abuse. P7 (PT) said, "I think VR devices and users can interact to exchange information, and third parties can abuse information."

Based on the quantitative results and qualitative results, we might say that our role-playing privacy tutorial (PT) could provide higher satisfaction than Privacy Policy. Also, we confirmed the result of analyzing qualitative data that PT could make a little bit of a privacy awareness change.

6 DISCUSSION & LIMITATION

This paper shows that the role-playing methodology for the Privacy Tutorial (PT) brings awareness to the users similar to the current Privacy Policy (PP) but with higher satisfaction and marginally better usability. The PT could expect efficacy and motivation in the real world. Because when working with mental workloads, the more diversely interactive environment of a VR rather than PCs positively impacts achievement and motivation [41].

There are several limitations that can be improved in future work. First, we recruited fewer subjects than the number of subjects recommended by the HCI community [3], which possibly led to the lower significance in the statistical analysis on usability and mental burden scores. We will derive more generalized results in future work with larger number of participants [3]. We also used a homogeneous sample with almost similar technical experience because participants were recruited from the local university. In future work, we need to recruit people with various backgrounds to adapt the research result to the real world. Second, several participants reported lower acknowledgment scores after experiencing the PP or PT; this might be due to their genuine thoughts, or their standards for the Likert scale were shifted. This phenomenon can be reexamined with a post-study survey showing pre-study survey results each participant submitted. Third, we made an artificial environment for the experiment. These could not generalize the situation where the user reads the original PP or plays PT using VR. Specifically, during our user study, participants who read PP were not allowed to do any more than reading the documents for their given time, which does not represent the natural interaction to PP. Finally, currently our PT was implemented without a proper systematic design method. We would use the iterative design method to improve the PT to make various and better prototypes in future work.

Our work examined the effectiveness of utilizing the role-playing method of presenting PP in VR. Our preliminary research showed that the role-playing method positively affected the user experience. We would further improve the poor user experience of PP in VR by conducting a more precise and in-depth study design in the future.

7 CONCLUSION

This work addresses the usability of role-playing methodology with a metaphor of physical embodiment for privacy tutorials of VR. We collected the mental models of experienced and inexperienced VR users regarding privacy and security issues. Interestingly, we found that even though most users knew their personal data are collected while using VR, no one could mention one VR-specific type of data not collectible from ordinary mobile devices. We also found that no experienced VR users had read their VR contents or devices' Privacy Policy (PP). We designed and implemented a role-playing privacy tutorial game based on the interview results where users can interact with virtual objects containing each type of VR data. Compared to the conventional text-based PP, our privacy tutorial could make users aware of the privacy issues as much as PP but higher satisfaction (p=0.007) and higher usability (with marginal significance p=0.11).

Considering the multi-modal and high dimensional nature of VR data, our work acknowledges the need for a more interactive and more accessible way to increase user awareness of how private information is collected from VR and utilized. Our formative study suggests that VR users might know less than their thoughts about what types of personal data VR devices can collect. We suggest a role-playing methodology may be utilized to aid this need and provide more improved satisfaction with less mental burden and difficulty of use than Privacy Policy.

ACKNOWLEDGMENTS

Our research was supported by the DGIST Start-up Fund Program of the Ministry of Science and ICT (2021010011).

REFERENCES

[1] Devon Adams, Alseny Bah, Catherine Barwulor, Nureli Musaby, Kadeem Pitkin, and Elissa M Redmiles. 2018. Ethics emerging: the story of privacy and security perceptions in virtual reality. In *Fourteenth Symposium on Usable Privacy and Security (2018)*. 427–442.

[2] Susanne Barth, Menno DT de Jong, Marianne Junger, Pieter H Hartel, and Janina C Roppelt. 2019. Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and informatics* 41 (2019), 55–69.

[3] Kelly Caine. 2016. Local standards for sample size at CHI. In *Proceedings of the 2016 CHI conference on human factors in computing systems*. 981–992.

[4] Caroline Cakebread. 2017. You're not alone, no one reads terms of service agreements. Retrieved November 28, 2020 from https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11.

[5] Zenobia C.Y. Chan. 2012. Role-playing in the problem-based learning class. *Nurse Education in Practice* 12, 1 (2012), 21 – 27. https://doi.org/10.1016/j.nepr.2011.04.008

[6] Tsai-Wei Chen and S Shyam Sundar. 2018. This app would like to use your current location to better serve you: Importance of user assent and system transparency in personalized mobile services. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–13.

[7] Thiam Kian Chiew and Siti Salwa Salim. 2003. Webuse: Website usability evaluation tool. *Malaysian Journal of Computer Science* 16, 1 (2003), 47–57.

[8] Kakao Enterprise Corp. 2019. Kakao Speech API. Retrieved December 17, 2020 from https://developers.kakao.com/docs/latest/ko/voice/rest-api#speech-to-text.

[9] Dana Craciun. 2010. Role-playing as a creative method in science education. *Journal of Science and Arts* 10, 1 (2010), 175.

[10] Ellysse Dick. 2021. *Balancing User Privacy and Innovation in Augmented and Virtual Reality.* Technical Report. Information Technology and Innovation Foundation.

[11] Kunal Gupta, Jovana Lazarevic, Yun Suen Pai, and Mark Billinghurst. 2020. AffectivelyVR: Towards VR Personalized Emotion Recognition. In *26th ACM Symposium on Virtual Reality Software and Technology.* 1–3.

[12] Marian Harbach, Markus Hettig, Susanne Weber, and Matthew Smith. 2014. Using Personal Examples to Improve Risk Communication for Security & Privacy Decisions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14).* Association for Computing Machinery, New York, NY, USA, 2647–2656. https://doi.org/10.1145/2556288.2556978

[13] Brittan Heller. 2020. *Reimagining Reality: Human Rights and Immersive Technology.* Technical Report. Carr Center Discussion Paper Series, June 12, 2020. https://carrcenter.hks....

[14] Yue Huang, Borke Obada-Obieh, and Konstantin Beznosov. 2020. Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems.* 1–13.

[15] Carlos Jensen and Colin Potts. 2004. Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems.* 471–478.

[16] Anna Jo and Brian Yongwook Chae. 2020. Introduction to real time user interaction in virtual reality powered by brain computer interface technology. In *ACM SIGGRAPH 2020 Real-Time Live!* 1–1.

[17] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. 2010. Standardizing privacy notices: an online study of the nutrition label approach. In *Proceedings of the SIGCHI Conference on Human factors in Computing Systems.* 1573–1582.

[18] Orin S Kerr. 2008. Criminal law in virtual worlds. *U. Chi. Legal F.* (2008), 415.

[19] David A Kipper. 1992. Psychodrama: Group psychotherapy through role playing. *International journal of group psychotherapy* 42, 4 (1992), 495–521.

[20] Tanja Kojić, Danish Ali, Robert Greinacher, Sebastian Möller, and Jan-Niklas Voigt-Antons. 2020. User Experience of Reading in Virtual Reality—Finding Values for Text Distance, Size and Contrast. In *2020 Twelfth International Conference on Quality of Multimedia Experience (QoMEX).* IEEE, 1–6.

[21] Tanja Kojić, Lan Thao Nugyen, and Jan-Niklas Voigt-Antons. 2019. Impact of Constant Visual Biofeedback on User Experience in Virtual Reality Exergames. In *2019 IEEE International Symposium on Multimedia (ISM).* IEEE, 307–3073.

[22] Richard L Levenson and Jack Herman. 1991. The use of role playing as a technique in the psychotherapy of children. *Psychotherapy: Theory, Research, Practice, Training* 28, 4 (1991), 660.

[23] James R Lewis and Jeff Sauro. 2009. The factor structure of the system usability scale. In *International conference on human centered design.* Springer, 94–103.

[24] Jie Li, Yiping Kong, Thomas Röggla, Francesca De Simone, Swamy Ananthanarayan, Huib de Ridder, Abdallah El Ali, and Pablo Cesar. 2019. Measuring and understanding photo sharing experiences in social Virtual Reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems.* 1–14.

[25] Facebook Technologies LLC. 2020. Oculus Terms of Service. Retrieved December 17, 2020 from https://www.oculus.com/legal/privacy-policy/.

[26] Ewa Luger, Stuart Moran, and Tom Rodden. 2013. Consent for all: revealing the hidden complexity of terms and conditions. In *Proceedings of the SIGCHI conference on Human factors in computing systems.* 2687–2696.

[27] Arnold M Lund. 2001. Measuring usability with the use questionnaire12. *Usability interface* 8, 2 (2001), 3–6.

[28] Philipp Mayring. 2019. Qualitative content analysis: Demarcation, varieties, developments. In *Forum: Qualitative Social Research*, Vol. 20. Freie Universität Berlin, 1–26.

[29] Ben Medler and Brian Magerko. 2010. The Implications of Improvisational Acting and Role-Playing on Design Methodologies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) *(CHI '10).* Association for Computing Machinery, New York, NY, USA, 483–492. https://doi.org/10.1145/1753326.1753398

[30] Edward F Melcer and Katherine Isbister. 2016. Bridging the physical divide: a design framework for embodied learning games and simulations. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems.* 2225–2233.

[31] Rory Mir and Katitza Rodriguez. 2020. If Privacy Dies in VR, It Dies in Real Life. Retrieved December 2, 2020 from https://www.eff.org/ko/deeplinks/2020/08/if-privacy-dies-vr-it-dies-real-life.

[32] Markus Montola. 2009. The invisible rules of role-playing: the social framework of role-playing process. *International journal of role-playing* 1, 1 (2009), 22–36.

[33] John William Nelson. 2011. A virtual property solution: How privacy law can protect the citizens of virtual worlds. *Okla. City UL Rev.* 36 (2011), 395.

[34] Ilesanmi Olade, Charles Fleming, and Hai-Ning Liang. 2020. BioMove: Biometric User Identification from Human Kinesiological Movements for Virtual Reality Systems. *Sensors* 20, 10 (2020), 2944.

[35] Fiachra O'Brolcháin, Tim Jacquemard, David Monaghan, Noel O'Connor, Peter Novitzky, and Bert Gordijn. 2016. The convergence of virtual reality and social networks: threats to privacy and autonomy. *Science and engineering ethics* 22, 1 (2016), 1–29.

[36] Wim TJL Pouw, Tamara Van Gog, and Fred Paas. 2014. An embedded and embodied cognition review of instructional manipulatives. *Educational Psychology Review* 26, 1 (2014), 51–72.

[37] Sara Price, Jennifer G Sheridan, and Taciana Pontual Falcão. 2010. Action and representation in tangible systems: implications for design of learning interactions. In *Proceedings of the fourth international conference on Tangible, embedded, and embodied interaction.* 145–152.

[38] Daniel Reinhardt, Johannes Borchard, and Jörn Hurtienne. 2021. Visual Interactive Privacy Policy: The Better Choice?. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems.* 1–12.

[39] Franziska Roesner, Tadayoshi Kohno, and David Molnar. 2014. Security and privacy for augmented reality systems. *Commun. ACM* 57, 4 (2014), 88–96.

[40] Young Sam Ryu and Tonya L Smith-Jackson. 2006. Reliability and validity of the mobile phone usability questionnaire (MPUQ). *Journal of usability studies* 2, 1 (2006), 39–53.

[41] Aili Shi, Yamin Wang, and Nan Ding. 2019. The effect of game–based immersive virtual reality learning environment on learning outcomes: designing an intrinsic integrated educational game for pre–class learning. *Interactive Learning Environments* (2019), 1–14.

[42] Julian Steil, Inken Hagestedt, Michael Xuelin Huang, and Andreas Bulling. 2019. Privacy-aware eye tracking using differential privacy. *Eye Tracking Research and Applications Symposium (ETRA)* (2019). https://doi.org/10.1145/3314111.3319915

[43] Hyewon Suh, Nina Shahriaree, Eric B Hekler, and Julie A Kientz. 2016. Developing and validating the user burden scale: A tool for assessing user burden in computing systems. In *Proceedings of the 2016 CHI conference on human factors in computing systems.* 3988–3999.

[44] Dag Svanaes and Gry Seland. 2004. Putting the users center stage: role playing and low-fi prototyping enable end users to design mobile systems. In *Proceedings of the SIGCHI conference on Human factors in computing systems.* 479–486.

[45] Madiha Tabassum, Abdulmajeed Alqhatani, Marran Aldossari, and Heather Richter Lipford. 2018. Increasing user attention with a comic-based policy. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems.* 1–6.

[46] European Union. 2016. General Data Protection Regulation. Retrieved January 11, 2022 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:FULL#d1e6191-1-1.

[47] Richard Warner and Robert Sloan. 2013. Scholarly Commons @ IIT Chicago-Kent College of Law Beyond Notice and Choice : Privacy , Norms , and Consent. January (2013).

[48] Ian Warren, Darren Palmer, et al. 2010. Crime risks of three-dimensional virtual environments. *Trends and issues in crime and criminal justice* 388 (2010), 1.

[49] Heng Xu, Hock-Hai Teo, and Bernard Tan. 2005. Predicting the adoption of location-based services: the role of trust and perceived privacy risk. *ICIS 2005 proceedings* (2005), 71.

[50] Richard Yao, Tom Heath, Aaron Davies, Tom Forsyth, Nate Mitchell, and Perry Hoberman. 2014. Oculus vr best practices guide. *Oculus VR* 4 (2014), 27–35.