Design of Privacy Indicators in Mixed Reality for Situationally Impaired Bystanders

SYED IBRAHIM MUSTAFA SHAH BUKHARI, Virginia Tech, USA
TIANYANG ROBIN LU, Virginia Tech, USA
AHMAD FARAZ KHAN, Virginia Tech, USA

Mixed Reality (MR) technologies are becoming more relevant especially with big technology giants like Apple and Meta developing their own MR headsets making them more available. However, as these MR headsets become mainstream, the privacy issues and concerns surrounding them materialize further as well and current privacy indicators are unable to address these privacy challenges due to their lack of accessibility especially for situationally impaired bystanders. Our research aims to address this gap in the literature. We conduct a focus group to brainstorm and propose 6 novel privacy indicators that better cater to situationally impaired bystanders. We then conduct a user study to evaluate the usability, usefulness in 8 different scenarios, and preferences of use for all proposed privacy indicators. To the best of our knowledge, this is the first work that addresses this gap in the literature as we propose key insights into design of future privacy indicators that cater to situationally impaired bystanders as well.

CCS Concepts: • **Security and privacy → Usability in security and privacy**.

Additional Key Words and Phrases: Privacy Indicators, Situational Impairment

ACM Reference Format:
Syed Ibrahim Mustafa Shah Bukhari, Tianyang Robin Lu, and Ahmad Faraz Khan. 2018. Design of Privacy Indicators in Mixed Reality for Situationally Impaired Bystanders . *ACM Trans. Graph.* 37, 4, Article 111 (August 2018), 7 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

Mixed Reality (MR) technologies – technologies that blend virtual content with the real world – are growing to be more relevant nowadays which has highlighted privacy concerns surrounding them. Technology giants have launched their own Mixed Reality headsets, like Apple's Vision Pro and Meta's Quest series, with varying pricing making MR technologies more available. While this has helped MR headsets become more mainstream, their mainstream usage also highlights the importance of addressing privacy concerns surrounding these devices [Guzman et al. 1970]. All of these headsets have many outward facing sensors, for example depth sensor, cameras etc., that continuously record the users and their surroundings. Prior research has shown that data being collected by MR headsets may be used to infer sensitive information like height, age, medical condition, mental state etc. [Miller et al. 2020] which can be used to identify people making the unsolicited data collection a significant privacy concern. However, collection of this data is integral to the functionality of these devices. Although the users may have some control over what data do these devices record of them, the privacy of bystanders - people present around the a device who are not actively using it - remains at risk. Hence, there is a need to inform bystanders whenever a MR device puts their privacy at risk.

Electronic devices in general, and MR devices specifically, make use of various privacy indicators to communicate their current state to the bystanders allowing them to be aware of their own privacy if the device is performing any action that puts their privacy at risk but they do not work universally for everyone or in every situation. A common privacy indicator that MR devices make use of is LEDs that visually convey the state of the device particularly to the bystanders. For example, MR headsets like Microsoft's HoloLens 2, Magic Leap 2, Meta's Quest Pro etc. make use of outward facing LED to visually communicate the status of the front facing camera to the bystanders. Other headsets like Apple's Vision Pro employ more creative ways to convey this information. It makes use of an outward facing display that shows the user's eyes when the user is not immersed in the virtual world letting the bystanders know that the user is able to look at them which makes the bystanders more aware of their own privacy. However, literature shows that current privacy indicators are not universally accessible [Sauer et al. 2010; Zhou et al. 2008]. This inaccessibility extends to bystanders who may find themselves in situations which do not allow them to notice, comprehend and reasonably act upon the privacy indicators.

We identify this inability of current privacy indicators to effectively address privacy concerns of situationally impaired bystanders as a gap in the literature and aim to address it with our research by asking the following research questions:

RQ_1: How can privacy indicators accommodate situationally impaired bystanders?

RQ_2: Why do situationally impaired bystanders prefer certain privacy indicators?

To answer RQ_1, we conducted a focus group with 8 participants, divided in 4 groups of 2, to brainstorm novel privacy indicators for MR headsets that are designed to cater for bystanders' situational impairment. The focus group resulted in 6 such novel privacy indicators. The focus group was followed by conducting user studies with 7 participants which helped us understand the usability of these proposed privacy indicators along with analyzing preference of their usage answering RQ_2. While we detail our findings in section 7 of the paper , here are our research's main contributions:

Authors' addresses: Syed Ibrahim Mustafa Shah Bukhari, Virginia Tech, Blacksburg, USA, simsb@vt.edu; Tianyang Robin Lu, Virginia Tech, Blacksburg, USA, robinlu@vt.edu; Ahmad Faraz Khan, Virginia Tech, Blacksburg, USA, ahmadfk@vt.edu.

ACM 0730-0301/2018/8-ART111
https://doi.org/XXXXXXX.XXXXXXX

(1) To the best of our knowledge, our research is the first one to address the research gap of designing privacy indicators to better cater situationally impaired bystanders.
(2) We propose six novel privacy indicators that are able to accommodate situationally impaired bystanders. We evaluate these privacy indicators for their usability and find them all to pass System Usability Scale's usability threshold.
(3) We provide insights to inform the design of future privacy indicators allowing them to better cater to situationally impaired bystanders.

2 RELATED WORK

2.1 Current privacy indicators

Some works such as [Windl et al. 2023] investigate security indicators for hyperlinking within the Metaverse. [Windl et al. 2023] identifies the need for security indicators in virtual reality (VR), given the rise of the Metaverse and its inherent security threats similar to those in web and mobile environments. Through in-depth interviews with domain experts and a user study involving the implementation and evaluation of five different security indicators, the study aims to understand the design dimensions for effective security indicators in VR. The findings highlight the effectiveness of visual indicators in the periphery for accuracy and task completion time, and a static visual indicator above portals for user preference due to its understandability and non-intrusiveness. Another work [Lin et al. 2023] explores suitable attributes and designs for conveying the authenticity of photorealistic avatars. [O'Hagan et al. 2023] conducts surveys to identify the extent to which bystanders' consent should be sought and the level of granularity of information necessary to provide awareness for AR devices. However, these very few works that do explore privacy indicators lack any consideration of situational impairment scenarios. These scenarios can make the existing privacy indicators proposed in these studies ineffective.

2.2 Inclusive privacy indicators

Very few works investigate the accessibility of privacy indicators. One such work [Zhao et al. 2023] explores privacy perceptions of bystanders with visual impairments (BVI) in the context of camera-based technology. Unlike previous studies that focused on the privacy concerns of visually impaired individuals as direct users of camera-based assistive technologies, this research explores their unique privacy perceptions and needs as bystanders, addressing a gap in existing literature. Through a preliminary survey and an in-depth interview study, the research highlights BVI's challenges in detecting camera use, their adapted privacy perceptions, empathy towards camera users with disabilities, and the complications faced in a sight-dominated world. It reveals BVI's unique concerns, including a lack of agency in detecting cameras, altered privacy expectations, high trust in acquaintances, and significant empathy for fellow disabled individuals using camera-based technologies for assistance. The study contributes to the understanding of BVI's privacy needs and suggests design considerations for future privacy-enhancing technologies tailored to their specific experiences and expectations. However, this study also only considers a single impairment scenario and does not consider the diverse set of situational impairment scenarios that we aim for with our work.

3 FOCUS GROUP METHODOLOGY

To gather ideas for novel privacy indicator systems that cater to situationally impaired bystanders, we elected to hold multiple focus group brainstorming sessions, amongst HCI researchers, in particular, those who have prior knowledge about the privacy and security concerns in MR. The focus groups were then tasked with generating ideas for privacy indicator systems that could function for situationally impaired bystanders.

3.1 Participants

We reached out to people through an email list of researchers. In total, 8 participants of various degrees of experience on the topic were recruited, with the most experienced ones being active MR technology users and researchers, and the least experienced ones having at least used MR headsets before, with some knowledge of the technology's potential privacy risks for bystanders. We decided against recruiting from the general population for the focus group portion of this study, since it requires some knowledge of the potential concerns and capabilities of MR technology, and the general population's knowledge of the topic were not deemed sufficient enough for designing new privacy indicator systems.

3.2 Procedures

Upon recruitment, participants were given a smaller introduction of the topic in their respective recruitment emails, in order to afford the participants the chance to prepare and fill any gaps in their knowledge on the topic of privacy indicators in MR, should they choose to. Each participant was also given a consent form to read and sign, notifying them of the purpose of the study, procedures to be followed, potential discomfort and risks, confidentiality policy, and the withdrawal policy, which allows them to terminate the session at any time, should they choose to. At the beginning of each official focus group session, the participants were given a primer presentation, introducing the key concepts of this focus group brainstorming session, including topics such as the bystander privacy issue, currently existing privacy indicator systems in MR, and definition of situational impairment, especially how they can potentially render the existing privacy indicator systems ineffective.

The focus group participants were then given the time to ask any questions and request clarifications for potential confusions on the topic introduced. After which, the participants were officially divided into groups of two, of their own pairing, and given pen and sketching papers to start a 30 minute period of discussion and designing in their respective groups. The participants were encouraged to discuss their ideas out loud, and sketch down any prototypes they think could be useful in the demonstration stage.

At the end of the 30 minute period, we notified the participants and asked them to give a presentation of their results in detail, explaining how they function, why they decided to make certain design choices, and how they can better benefit bystanders that are situationally impaired. All participants shared their results, mostly

with two privacy indicator systems each, with the exception of one group that only provided one final result. During the demonstration, we recorded their answers and asked clarification questions on the details of each system, eventually giving us a total of 7 privacy indicator systems, which will be discussed in the following section.

4 FOCUS GROUP RESULTS

In this section, we will discuss the resulting bystander privacy indicator systems for situationally impaired bystanders that our focus groups generated. Some of the ideas from the focus groups were similar, despite being from separate focus groups and sessions. We have consolidated the ones that were functionally similar into one system. Through this process, we finalized a set of 6 bystander privacy indicator systems. Some are similar in ways they function, but upon consideration, the way they trigger are different enough that could warrant a significant difference in both usability and user preferences, which is why they were kept as separate systems. Following is the set of 6 bystander privacy indicator systems, written in the same format that is eventually presented to our user study participants.

4.1 HMD with Static Display System

Imagine MR headsets having a big outward facing screen that covers the entirety of the front of the headset. Every time the user of the headset records anything, a neon-sign indicating the activity being performed by the user shows up on the entire screen letting bystanders know that they are being recorded.

4.2 HMD with Dynamic Display System

Imagine MR headsets with a big outward facing screen that covers the entirety of the front of the headset. Every time the user of the headset is recording anything, a real time display that mirrors what the user is recording will be shown on the outward display. An additional display will be on the side with all the faces that were captured this way in the last 1 minute.

4.3 Proximity Activated Phone Notification System

Imagine MR headsets are connected to all smartphones such that every time a headset starts recording, all smartphones in the vicinity receive a notification (with audio, visual and haptic feedback) indicating that a headset nearby is recording. Each user can set their notification preference for this notification on their smartphone.

4.4 Gaze Activated Phone Notification System

Imagine an MR headset system which tracks gaze data and sends a notification to bystanders if they are being stared at. The notification will be an air-tag like system that will send a mobile notification to the bystander's mobile device.

4.5 Hand Gesture Permission System

Imagine that all MR devices can blur out Bystanders faces from being recorded or shown if they have not provided permission. The Bystanders can provide and remove permissions of being recorded by using a hand gesture.

4.6 Activity Aware Adaptable Notification System

Imagine MR headsets with outward displays, when the headset wearer has the camera feature enabled, regardless of activity, a small light will be displayed; when the headset starts recording, a bigger, blinking light will appear, with a repetitive tone from the speaker; when the camera is recording and a human face is detected, the light will be start flashing, and the sound will become louder.

5 USER STUDY METHODOLOGY

In this section, we will discuss how the user study portion of the study is conducted. We conducted a survey study to understand the usability of each bystander privacy indicator system, how each bystander privacy indicator system functions in scenarios of different privacy stakes and impairment levels, as well as the user preferences for each system and the reasons for them.

5.1 Participants

For the user study portion, we chose to recruit participants from a different population than the focus group. We sent out recruitment emails through the Virginia Tech listserv, to both undergraduate and graduate students, which collected the email addresses, degree level, and prior experiences with MR devices, which range from no experiences at all, to very familiar. While our initial intent was to survey participants of experience levels, we decided to exclude participants with no experiences in MR at all in the final selection stage, since we concluded that having no experiences in MR will be detrimental to accurately evaluate the bystander privacy indicator system, and that at least some prior experiences will be required. We also initially aimed for 12 participants for our user study, but due to scheduling issues and various time constraints, only 7 were able to participate, with 4 being undergraduate students, and 3 being graduate students, of which, 3 reported being somewhat familiar with MR devices, 2 reported being familiar with MR devices, and 2 being very familiar with MR devices. We also excluded all recruitment responses from previous focus group participants, in order to reduce biases they would have on systems they proposed themselves.

5.2 Procedures

During the user study, each participant was first assigned a randomized participant ID that is not tied to their name or email address, ranging from P01 to P33, to maintain our participants' anonymity and protect their identity. Each participant was also given a consent form to read and sign, notifying them of the purpose of the study, procedures to be followed, potential discomfort and risks, confidentiality policy, and the withdrawal policy, which allows them to terminate the session at any time, should they choose to.

At the beginning of each user study session, the participant was given a primer presentation, introducing the key concepts of this study, including topics such as the bystander privacy issue, currently existing privacy indicator systems in MR, and definition of situational impairment, especially how they can potentially render the existing privacy indicator systems ineffective. The participant was then given time to ask any questions and request clarifications for potential confusions on the topic introduced. Upon the conclusion

of this section, the participant was asked to fill out a survey, which has multiple sets of questions that will be explained below.

It is worth noting that, in the way the survey is structured, there are a total of 7 sections, with the first 6 each being dedicated to one bystander privacy indicator system with identical questions, in which we first present the participant with a bystander privacy indicator system, as per the results of the focus group sessions, we then answered any question and clarification requests from the participant, after which, we asked the participant to rate the usefulness of the system given a certain scenario, and a set of System Usability Scale questions to evaluate the usability of the system. In the last section, a recap of all bystander privacy indicator systems was provided, and the participant was asked to provide an overall ranking of all involved systems, as well as their reasoning.

5.2.1 Scenarios. In the scenario specific questions, the participant was asked to rate the usefulness of the given system on a five point scale, ranging from not very useful, to very useful, based on how useful the bystander privacy indicator system will be in the given scenario, with different degrees of situational impairment, as well as different levels of stakes in privacy. There are a total of 8 scenarios, of which 4 are indoor, 4 are outdoor. They are listed below.

- Scenario 1: You're in a classroom, sitting and waiting for your professor to show up, a classmate is recording a video with their headset.
- Scenario 2: You're in a classroom, taking an open book exam, a classmate is recording a video with their headset.
- Scenario 3: You're in a park, sitting and relaxing on a bench, a person nearby is wearing a headset and recording a video.
- Scenario 4: You're in a park, reading a book, a person nearby is recording a video.
- Scenario 5: You're in a bank, waiting for your turn at the teller register, a person beside you in the line is recording a video with their headset.
- Scenario 6: You're in a bank, filling out a form with your personal information, and another person sitting beside you is recording a video with their headset.
- Scenario 7: You're on a beach, sunbathing on a beach chair, and a person sitting beside you is recording a video with their headset.
- Scenario 8: You're on a beach, playing volleyball, and a person who is watching the match is recording a video with their headset.

In all of the provided scenarios, the participant was asked to rate the usefulness of the system, assuming the role of a bystander, during which a person nearby is wearing a MR device with the described bystander privacy indicator system.

5.2.2 System Usability Scale (SUS). In each section for a bystander privacy indicator system, the participant was asked to fill out a System Usability Scale questionnaire, which has a 5-point scale ranging from strongly disagree to strongly agree with the statements. The SUS results are then used to evaluate the usability of each system, to ensure these novel systems all meet an acceptable level of usability requirement. The language of the questionnaire is slightly modified to accommodate for the fact that the participant will not have used the system at this point and is basing decisions on descriptions and what they believe it would be like for them. The exact questions will be shown below as listed.

(1) I think that I would like to use this system frequently.
(2) I find this privacy indicator unnecessarily complex.
(3) I think this privacy indicator is easy to use.
(4) I think that I would need the support of a technical person to be able to use this privacy indicator.
(5) I find the various functions in this privacy indicator to be well integrated.
(6) I think there is too much inconsistency in this privacy indicator.
(7) I would imagine that most people would learn to use this privacy indicator very quickly.
(8) I find this privacy indicator very cumbersome to use.
(9) I feel very confident using this privacy indicator.
(10) I need to learn a lot of things before I can get going with this privacy indicator.

All the results from the questionnaire are then collected and calculated according to standard. Item 1,3,5,7,9 are scored positively, with item 2,4,6,8,10 being scored negatively, the values were then calculated with a standardized score to represent the overall usability of the system.

5.2.3 Preference Ranking. In the last section of the survey, we present the participant with an overview of the 6 bystander privacy indicator systems they have evaluated. We then asked the participant to rank them on the basis of their preference of usage as a bystander, for general use case, with a score of 6 being the highest ranking, and 1 being the lowest ranking, this step is then repeated, with the difference of how they would rank it, if it is from the standpoint of someone as a situationally impaired bystander.

The rankings were then followed by questions that ask the participant to elaborate on their reasoning behind their ranking decisions, one for why the highest ranking one was selected, and one for why the lowest ranking one was selected, which again, is repeated for their decisions for situationally impaired bystanders. At the very end of the survey, we presented a free response question which collected any thoughts, feedback, or comments the participant had during the user study.

6 USER STUDY RESULTS

6.1 Average System Usability Scores

To ensure that the proposed privacy indicators from the focus group are usable, we administer System Usability Scale (SUS) as a quality control and get the SUS score of each privacy indicator from all user study participants. In Figure 2, we plot these SUS scores for each indicator averaged across all participants to evaluate their overall usability. We observe that privacy indicators 3 and 4 have the best usability amongst the proposed privacy indicators while 2 has the least usability. We note that all of the proposed privacy indicators, even the least usable one, have a SUS score greater than 50 which is the threshold between usable and not-usable system according to SUS. This shows that all the proposed privacy indicators are usable passing our quality control.

6.2 Average Perceived Usefulness Per Scenario

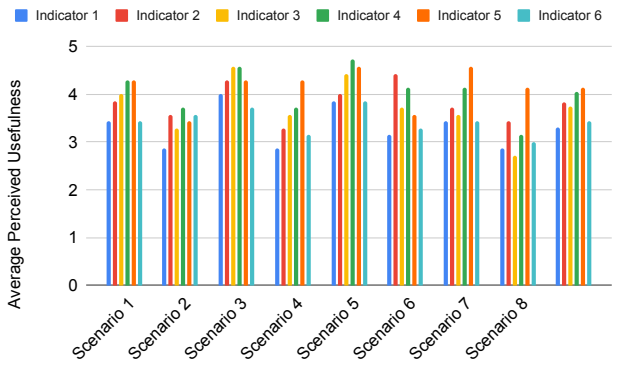

Fig. 1. Average perceived usefulness per scenario.

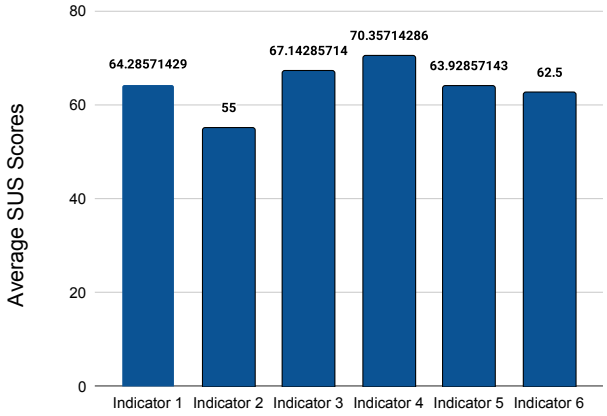

Fig. 2. Average system usability scores (SUS).

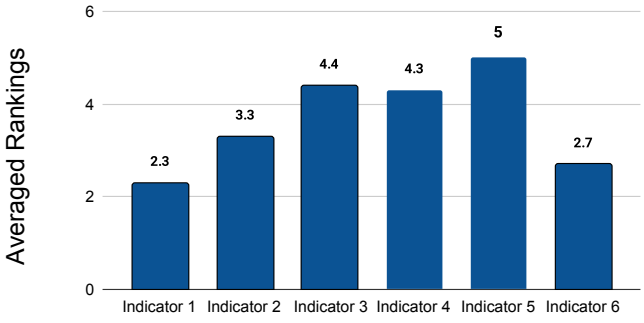

Fig. 3. Rankings of PIs under non-situationally impaired conditions.

Analysis of the user study results specifically the perceived usefulness per scenario suggests that the perceived usefulness is higher

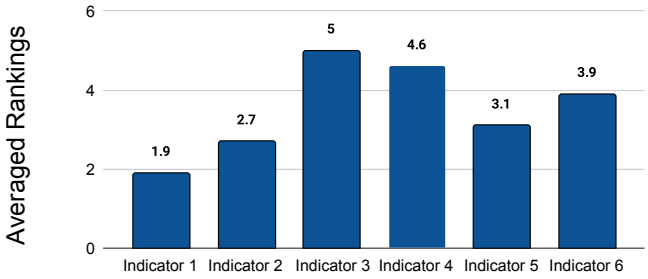

Fig. 4. Rankings of PIs under situationally impaired conditions.

in general for scenarios where the need for privacy is low and the impairment level is also low. This can be observed in Figure 1 for scenarios scenario 1, 3, and 5, in which both of these conditions are true. In contrast, for scenarios 2, 6, and 8 as seen in Figure 1 where the need for privacy is high and impairment level is also high, the perceived usefulness is lower in general.

One likely reason for this behavior is that when the need for privacy and the impairment level are both low, users presume that most of the privacy indicators will be useful as they will be easier to notice. Thus, when privacy and impairment are low, people are not too critical of privacy indicator systems hence overall higher perceived usefulness but as soon as privacy and impairment become high, people become more critical of the privacy systems and their ability to address this high privacy and impairment level. Hence, both these observations highlight an inverse relation between impairment level and the need for privacy with perceived usefulness.

Another observation from the averaged rankings of indicators from the User Study as shown in Figure 1 is that Indicator 4 consistently stays in the top 2 for perceived usefulness across all scenarios. This observation is consistent with SUS scores for usability as well as shown in Figure 2 where Indicator 4 has the highest score.

6.3 Ranking on Preference of Use

Upon reaching the last section of the user study, participants were surveyed for their rankings of the bystander privacy indicators, on the basis of their preference of use, as well as their reasonings. The results were divided into two categories, one for general use, from the perspective of non-situationally impaired bystanders (see Figure 3), one from the perspective of situationally impaired bystanders (see Figure 4), which are both used in the analysis following.

The participants were asked to rank all six bystander privacy indicator systems, with 6 representing the highest ranked. The results are then averaged across all participant responses. Amongst the data, we observed some interesting changes between the two sets. The first of which being the change in ranking of certain bystander privacy indicator systems, while initially ranked only 5th in general use, for non-situationally impaired bystanders, indicator 6, the Activity Aware Adaptable Notification System rises the most in ranking and reaches 3rd in ranking for situationally impaired bystanders; conversely, indicator 5, the Hand Gesture Permission System, lowers from 1st place for non-situationally impaired bystanders in ranking to 4th place for situationally impaired bystanders. The rest of the

rankings only changed the maximum of 1 place, which we consider to be not significant enough for analysis.

We found the change in ranking for indicator 6 and indicator 5 to be enough to warrant a closer examination. Initially, indicator 6, the Activity Aware Adaptable Notification System was ranked quite low for non-situationally impaired bystanders, this system uses a combination of visual and audio cues to notify bystanders, which progressively gets more noticeable as the activity becomes more privacy invasive, with the maximum level being activated upon detection of human faces being recorded, emitting a flashing light and a repetitive loud sound. When examining the reason that was given for why they ranked indicator 6 the lowest, participant P02 commented that "*it is very awkward when people are recording and you can hear the voice(audio cue) getting louder and louder*", participant P06 commented that "*the repetitive tone from a speaker might be annoying to deal with*", participant P32 described it as a "*unnecessary disturbance*". However, when considering the same ranking for situationally impaired bystanders, participants ranked indicator 6 higher, and when examining the reasons behind it, participant P23 commented that "*From the perspective of a busy bystander this indicator would redirect my attention most easily*", participant P33 commented that "*with the flashing lights and the loud speaker, it's hard to imagine ignoring the user recording*".

From the comments collected, we deduced that despite indicator 6 not being most preferred initially for non-situationally impaired bystanders, due to it being potentially disruptive and intrusive, this opinion quickly changes when situational impairment is introduced and the more subtle privacy indicator systems start to face the problem of not being noticed at all, and people show willingness to sacrifice some of the subtlety of the system to ensure privacy and functionality, making it more acceptable.

On the other end of the spectrum, we examine indicator 5, the Hand Gesture Permission System, which allows bystanders to use a simple hand gesture to give or revoke permission of recording, and automatically blurs out faces unless given permission. When asked for their reasoning behind the ranking for non-situationally impaired bystanders, participant P25 commented that "*it allows more control since I'm able to blur my face using hand gesture*", participant P24 commented that they prefer it because "*My privacy is taken care of itself*", participant P32 commented that "*it respects the privacy of bystander the most and allows the bystander to dictate if they want to be blurred out if they are not comfortable with it*", participant P33 commented that "*indicator 5 makes the most sense in terms of realism*". This also changes, however, when situational impairment is introduced, when asked for their reasons for the new ranking, participant P06 commented "*even though I myself should be blurred out, I would still not know whether I was considered a bystander or not*", citing the uncertain nature of the automatic blurring system.

From the comments collected, we found that while generally preferred for non-situationally impaired use cases, participants were much concerned with the reliability of indicator 5, which requires the bystander to be visually aware of the MR device user to use hand gesture for giving or revoking permission, which may not be possible if they're situationally impaired, at which point it mostly falls back to automatic blurring system. The participants indicated a general distrust of letting an automatic software system handle the face blurring and privacy protection, this mistrust also extends to the device manufacturer that they may not have the user's best interest as the top priority.

It is also worth noting that, across the two sets of rankings, indicator 1, the HMD with Static Display System was consistently ranked the lowest, with participant P23 commenting "*if I'm at a distance from the person recording, I cannot see their screen*", and participant P25 commenting "*it only tells me that someone is recording without providing me information on what they're recording or giving me control to stop them from recording me*". When considered for situational impairment, more participants ranked indicator 1 as the lowest, participant P06 commented "a neon sign is easily unnoticeable", and "*it is easy to not notice it if I'm occupied with something else*", participant P33 commented "*although neon makes it stand out, in comparison to everything else I feel like it would be the less blatant indicator out of the 6*". It is concluded that the singular modality nature of indicator 1, as well as the lack of control options for bystanders make it overall the least preferred bystander privacy indicator. It is also worth noting that indicator 1 is also the one that is closest to currently existing bystander privacy indicators on commercially available headsets at the time of writing, indicating a potential need for new bystander privacy indicator systems.

7 CONCLUSION

In this study, we started by conducting a literature review on currently existing bystander privacy indicator systems. We found that there is currently a gap in existing literature on bystander privacy indicators that can accommodate situationally impaired individuals. We then conducted focus groups and proposed 6 novel bystander privacy indicator systems. Each system was evaluated in a following user study for its usability, usefulness in different scenarios, and preferences of use, which will be discussed in sections below.

7.1 Discussion

We can also observe an interesting phenomenon regarding the correlation between perceived usability and preference ranking of indicators from results in Figures 2, 3, and 4. It can be observed that even though the SUS score of Indicator 1 is among the top three, it is still not ranked well as a preferred indicator in Figures 3, and 4. This goes to show that if an indicator has a higher usability it does not necessarily mean that it will be preferred so any new privacy indicator should be evaluated for both the metrics.

Another interesting observation is that indicators 3 and 4 are consistently highly ranked for both usability and preferences. One property that both these indicators share is that they are similar in terms of functionality which is a notification-based system. Since notifications are a common medium of alerts in mobile devices we speculate that they are manipulations of existing and known systems that people are familiar with and can imagine easily, so people find them more usable and also prefer these indicators. Another likely reason is that phone notification systems allow bystanders to have control over how they want to be notified making them more preferred over other indicators which do not have that flexibility.

7.2 Limitations

Despite observing some interesting results as discussed in section 7, we acknowledge the limitations that we faced in our research. A major limitation that we encountered stems from the short time we had to execute the project which resulted in the user studies having a limited sample size of 7 participants. The impact of this limitation is most evident from our failure to observe any meaningful trends while looking at average perceived usefulness of the perceived indicators for specific scenarios.

Another limitation that we observe is in our study design where we do not sketch or prototype any of the proposed privacy indicators for our user study participants to see or experience before evaluating them. Although we provide detailed descriptions of each proposed privacy indicator, we believe that relying on description alone may not have been effective in ensuring that the participants understand the proposed privacy indicators well. Hence, there may have been individual biases of participants in the evaluation of the proposed privacy indicators due to differences in interpretations of the provided descriptions for each proposed privacy indicator.

Finally, we rely on System Usability Scale's threshold of usability value of 50 [Soegaard 2024] to determine if the proposed privacy indicators are usable or not. Prior literature shows the average usability value to be 68 [Hyzy et al. 2022] while the value of 70 is considered to be a good usability score [Soegaard 2024]. This renders the value of 50 to be a low usability threshold. We believe that the lack of sketches or prototypes might have resulted in overall low usability scores for our proposed privacy indicators as rating a privacy indicator relying solely on a description of it could have been tricky for the user study participants.

7.3 Future Work

Our work can be extended in the future while addressing the limitations identified in section 7.2. Any future work should address the methodological limitation of prototyping or sketching the proposed privacy indicators so that the participants are able to see or experience the proposed privacy indicators. This would result in a more realistic scoring by the participants of each privacy indicator's usability as well as their preferences for each.

Additionally, prototyping the proposed indicators makes a case for possible future implementation which may help participants evaluate them solely on their usability and ability to cater to situationally impaired bystanders rather than questioning their practicality. Doing so combined with increasing the sample size of the user study would result in more interesting, more generalizable trends which our research was unable to observe particularly for scenario specific perceived usefulness of each proposed privacy indicator. Increased sample size would also help establish statistical significance of any observed trends for future studies in this domain.

REFERENCES

Jaybie A. De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. 1970. Privacy and security issues and solutions for mixed reality applications. https://link.springer.com/chapter/10.1007/978-3-030-67822-7_7

Maciej Hyzy, Raymond Bond, Maurice Mulvenna, Lu Bai, Alan Dix, Simon Leigh, and Sophie Hunt. 2022. System usability scale benchmarking for digital health apps: meta-analysis. *JMIR mHealth and uHealth* 10, 8 (2022), e37290.

Jinghuai Lin, Johrine Cronjé, Carolin Wienrich, Paul Pauli, and Marc Erich Latoschik. 2023. Visual Indicators Representing Avatars' Authenticity in Social Virtual Reality and Their Impacts on Perceived Trustworthiness. *IEEE Transactions on Visualization and Computer Graphics* 29, 11 (2023), 4589–4599. https://doi.org/10.1109/TVCG.2023.3320234

Mark Roman Miller, Fernanda Herrera, Hanseul Jun, James A Landay, and Jeremy N Bailenson. 2020. Personal identifiability of user tracking data during observation of 360-degree VR video. *Scientific Reports* 10, 1 (2020), 17404.

Joseph O'Hagan, Pejman Saeghe, Jan Gugenheimer, Daniel Medeiros, Karola Marky, Mohamed Khamis, and Mark McGill. 2023. Privacy-Enhancing Technology and Everyday Augmented Reality: Understanding Bystanders' Varying Needs for Awareness and Consent. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 6, 4, Article 177 (jan 2023), 35 pages. https://doi.org/10.1145/3569501

Graig Sauer, Jonathan Holman, Jonathan Lazar, Harry Hochheiser, and Jinjuan Feng. 2010. Accessible privacy and security: A universally usable human-interaction proof tool - universal access in the information society. https://link.springer.com/article/10.1007/s10209-009-0171-2#citeas

Mads Soegaard. 2024. System usability scale for data-driven UX. https://www.interaction-design.org/literature/article/system-usability-scale#:~:text=*%202.5%20=%2082.5.-,6.,score%20above%2085%20is%20excellent.

Maximiliane Windl, Anna Scheidle, Ceenu George, and Sven Mayer. 2023. Investigating Security Indicators for Hyperlinking Within the Metaverse. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. USENIX Association, Anaheim, CA, 605–620. https://www.usenix.org/conference/soups2023/presentation/windl

Yuhang Zhao, Yaxing Yao, Jiaru Fu, and Nihan Zhou. 2023. "If sighted people know, I should be able to know:" Privacy Perceptions of Bystanders with Visual Impairments around Camera-based Technology. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 4661–4678. https://www.usenix.org/conference/usenixsecurity23/presentation/zhao-yuhang

G. Zhou, J. Lu, C.-Y. Wan, M. D. Yarvis, and J. A. Stankovic. 2008. *Body Sensor Networks.* MIT Press, Cambridge, MA.