Evaluating bystander privacy in MR systems

Kenneth Pat
patk@uci.edu

Kurtis Chow
kurtishc@uci.edu

Mohanapriya Singaravelu
singaram@uci.edu

Waleed Helal M Alharbi
whalharb@uci.edu

Abstract

With rapidly advancing virtual, augmented, and mixed reality (MR) devices, which will one day become commonplace like smartphones, the privacy of not just the users but also the people around them becomes important. These devices use numerous sensors for their functionality but inadvertently capture data from the bystanders.

This paper focuses on evaluating bystander privacy in MR systems. We followed a 2-phase methodology to first understand the users and translate the learnings to evaluate existing solutions in literature. Through a survey, we answered our first research question on whether users are aware of privacy attacks in MR and how they respond to it. 38% of the participants were aware of some of the privacy breaches. Most of the participants were concerned by these issues, which increased when the user was a stranger. The evaluated solutions satisfy the concerns related to camera data. Other kinds of sensors were not addressed. Our recommendations for this area would be to develop a privacy framework that addresses all types of privacy attacks.

1 Introduction

In recent years, augmented reality (AR), virtual reality (VR), and mixed reality (MR) technologies have gained significant popularity. With the growing demand for AR and MR devices, many leading technology companies have developed their own AR and MR headsets. However, this rapid expansion of AR and MR devices has introduced numerous concerns related to usable security and privacy. These headsets typically feature various sensors, such as cameras and microphones, that collect users' personal data, including audio and video. This data collection raises critical questions about how these devices handle privacy and security. To address these concerns, our project focuses on understanding and mitigating privacy threats posed by MR devices through a user study on bystander privacy.

Previous research highlights that MR technologies rely heavily on sensors to gather real-time, context-specific personal information, which creates significant privacy risks. Participants in prior studies have expressed concerns about app permissions that enable their personal data to be accessed and shared with developers. In response to such issues, some MR devices, like the Quest, have restricted developers from accessing cloud data, emphasizing the industry's growing attention to privacy concerns [11] [12].

Our study specifically examines the privacy implications for bystanders who may be recorded or monitored by MR devices without their consent. We conducted surveys to collect firsthand feedback from participants and reviewed existing literature to evaluate solutions proposed in prior research. This work aims to identify effective strategies to protect bystanders from the unintended privacy risks associated with MR device use. [11] [12].

2 Background and Related Work

2.1 MR Devices

Today's mixed reality (MR) tools come in various forms. The most common are head-mounted displays (HMDs), such as the Meta Quest and Apple Vision Pro. Surprisingly, even mobile devices, such as those used in apps like Pokémon GO, represent a form of MR entertainment. Beyond entertainment, MR tools include heads-up displays (HUDs), which are integrated into jets and some cars, and specialized systems like CAVE, which create immersive 3D environments using projectors or LED screens. For this paper, however, we focus on the security and privacy concerns of HMDs due to resource constraints.

HMDs rely on three primary tracking types: pose tracking, eye tracking, and finger tracking. These methods work together to gather detailed information about users and their surroundings, maintaining the illusion of virtual entities and enhancing device performance.

Pose tracking determines a user's orientation and position. Common methods include cameras integrated into the HMD [5], external cameras [16], accelerometers, gyroscopes,

or magnetometers for orientation [4], and acoustic methods similar to echolocation [15]. A widely adopted approach is sensor fusion, which combines multiple sensor outputs to produce superior results. This study focuses on optical sensors, accelerometers, and gyroscopes due to equipment limitations and their prevalence.

Eye tracking is often conducted via cameras with varying levels of physical intrusion. Some systems rely on corneal and pupil reflection, while others monitor the front and back lenses or the interior of the eye [7]. More invasive methods place cameras inside the eye, but these fall outside the scope of this study. Non-optical approaches to eye tracking exist but are also excluded from our analysis.

Finger tracking generally employs two methods: interfaces like motion controllers or sensors such as cameras. Early HMDs used motion controllers to track hand and finger movements for activities like gaming. These controllers leverage a combination of technologies, including inertial measurement sensors, cameras, or markers for optical tracking, and magnetometers to monitor magnetic fields generated by a base station [1].

By integrating these sensors with advanced algorithms and machine learning models, HMDs can collect extensive data about a user's 3D environment, behavior, and even bystanders'. While individual sensors may seem basic, the combination of data from these inputs raises significant privacy and security concerns.

HMDs predominantly use optical sensors (internal or external) to track hands, eyes, and positioning [2], while accelerometers and gyroscopes capture rotation and orientation. Our study will focus on how these sensors collect and transform data. Although substantial research exists on securing MR devices, including through spatial recognition [18], we aim to build upon these findings while ensuring a diverse and unbiased review of related work.

2.2 Related Work

In researching this topic, we reviewed several papers on securing MR-specific features. One study proposed PrivacEye [18], a novel method of closing the shutters on MR device's cameras using eye-tracking. Additional papers discussed threat models tailored to MR or vulnerabilities, such as front-facing cameras and spatial data collection.

O'Hagan et al. [17] is a paper on this topic that performed a survey to capture "bystanders' awareness of, and concerns regarding, potentially privacy infringing AR activities; the extent to which bystanders' consent should be sought; and the level of granularity of information necessary to provide awareness of AR activities to bystanders." The paper surveys 102 participants and provides amazing insights into bystanders' awareness and concerns towards AR devices, which differ from MR in not introducing digital elements that interact with the real world. However, the paper does not explore existing solutions, both in-use and proposed, on the topic. Our paper hopes to expand on their work through our analysis of existing and proposed solutions with our survey's conclusions.

Another paper by De Guzman et al. [8] performs a literature review of different proposed solutions. They note several challenges and extend their research to privacy solutions in related fields. Papers were categorized by combining models from three prior papers. However, none of these papers try to apply these models nor use information gathered from real bystanders. Our work hopes to address this weakness by utilizing real awareness and concern to inform a review of a privacy solution.

Both papers provide a component of this paper research: O'Hagan et al. is a survey gathering bystanders' awareness and concern and de Guzman et al. examines different solutions. Our paper hopes to combine the components of both to provide a more practical analysis of proposed solutions.

3 Methodology

Our study focuses on two key aspects. First, we assess the general user perception and awareness of privacy concerns in MR systems through a user study (survey). Second, we will conduct a comparative analysis of different solutions that address the bystanders privacy. The user study provides insight into how participants feel about certain types of attacks and attackers. These results inform us if they believe these solutions adequately address their concerns.

Our goal is to answer the following research questions:

RQ1: To what extent are users aware of privacy issues in Mixed Reality (MR) systems, and how do they perceive and respond to these concerns?

RQ2: What are the most effective solutions for protecting bystander privacy in MR environments, and how do these solutions compare in terms of user acceptance and efficacy?

3.1 Hardware and Recordings

We discovered that the ANTrepreneur Center at UC Irvine has Apple Vision Pros for students to try. According to sources, it consists of approximately 300 components, including five sensors, six microphones, and twelve cameras [3]. It also has sensors that are found in most smartphones like accelerometers and gyroscopes. We booked a demo session and recorded videos demonstrating Apple Vision Pro's main features and functionalities. We presented these videos in the survey to familiarize the participants with the tool.

Since none of us are familiar with the recording process on Apple Vision Pro, we asked Tanis Sarbatananda, an undergraduate student who works at the ANTrepreneur Center to

assist us with the process. We recorded five videos with a total length of 9 minutes and 30 seconds, which covered various categories of applications available on the device: three 3D gaming apps, one health app, and one drawing app. We aimed to select as many apps as possible to let our survey be more comprehensive and representative. However, due to the time constraints of our project, we had to limit the total length of all recordings to less than 10 minutes, in order to let the participants finish our survey in a reasonable time.

3.2 User Survey

3.2.1 Recruitment

Due to time considerations, recruitment was predominantly from friends, family and the student body at UC Irvine. We also tried to recruit from Discord, Reddit and WhatsApp. Participants were expected to be at least 18 years old or associated with UCI, located in the US and fluent in English. These conditions were primarily to meet the IRB requirements for user studies.

3.2.2 Survey Design

Our user survey was largely based on the one presented by O'Hagan et al [17]. Their survey presented different types of attack that future devices could be capable of. We specifically selected ones we felt were more realistic or were already real. We used the following types of MR privacy attacks, definitions taken from O'Hagan et al [17]:

- *Camera Usage:* An application generally using the camera(s) on the device
- *Microphone Usage:* An application generally using the microphone(s) on the device
- *Volumetric Capture:* Capturing 3D imagery that could later be viewed or repurposed (e.g. a 3D model of your body or home)
- *Bio-Metric ID:* Identifying who other people are (e.g. through facial ID or other biometric data)
- *Activity Tracking:* The physical movements, behavior and activity of nearby people
- Personal Characteristics: Identifying and inferring personal characteristics of other people such as gender identity, age, race, sexuality etc
- *Augmented Appearance:* Augmenting or altering others appearance (e.g. applying snapchat or instagram-like filters to your view of others) - pertaining to altered reality as applied to people.

Our survey first asks if participants were eligible and then if they were fine with what information the survey would collect. Anyone who answered "Yes", to both, was then presented with the full study. Otherwise, the survey would be immediately terminated.

After accepting the terms, they were asked a few demographic questions about their age, gender, and education. The question on age asked which generation they fell into according to a categorization made by Pew Research Center in 2019 [10]. For gender, they were given the following options: *male*, *female*, *non-binary,* and *the option to be exempt*.

After the demographic section, they were asked questions about their prior experience with mixed reality devices. Some questions included virtual reality and augmented reality as options. They also included what they used the device for if they have any experience.

They were then presented the aforementioned video to familiarize them with an MR device. The video is around ten minutes long and demonstrated several features such as virtual displays, changing the environment, and introducing digital objects. The video is expected to familiarize them with the capability of MR devices to contextualize the following section.

A series of scenarios associated to each type of privacy attack were presented to them. Each scenario was designed to introduce a type of privacy attack a bystander could receive with minimal bias. After reading through them, they were asked questions on each type of attack. Questions included measured if they were aware of the attack, if their level of concern changes depending on the attacker(family v. friend v. acquaintance v. stranger) or type, and what sort of solution they would prefer in the event of an attack. Options for a question were generally presented either as a value between *Strongly Agree* and *Strongly Disagree* or how they would like their permission to be considered by the MR device(*"Opt-out - I would never consent to this activity"*, *"Opt-out by default, with ability to request your consent"*, *"Opt-in by default, with ability to withdraw your consent"*, and *"Opt-in by default, no consent required"*). Notably is an awareness question prior to the scenarios. Its inclusion and a similar question after the scenarios act as a measuring stick of inconsistency in participant's responses and to measure if our scenarios biased them.

Lastly, they were asked about if the new knowledge has affected their concern and final comments about the survey itself.

3.2.3 Pilot Study

A pilot study was performed prior to the full study. Five participants completed the survey and their responses were used to calculate Cronbach's Alpha. Its alpha was 0.8, indicating internal consistency across the questions. However, there were critiques on the survey's length, one participant noting

it took them forty minutes. We remedy this by presenting all the scenarios at once and combining identical questions into a grid format. Aside from these structural changes, the survey is largely unchanged.

3.3 Paper Analysis

For the second aspect, we reviewed several of the papers, discussing different methodologies to tackle MR's unique security concerns for bystander privacy and evaluate which performs the best overall.

We evaluated two main categories of bystander privacy solutions:

1. **Explicit Systems:** These methods have the option to let the users or bystanders decide the privacy measures to be taken. This includes approaches where bystanders are pre-determined, such as training models on bystanders' images, using facial signatures, requiring special equipment worn by bystanders, or detecting bystanders via hand gestures and eye-tracking [18].

2. **Implicit Systems:** In these approaches, no action is required by the user or bystanders. The system automatically detects and prevents the recording of bystanders. Solutions typically involve ML models that detect eye movements or use voice recognition.

The starting point of our research was understanding the field by reading literature surveys by other authors [8] [17] [9]. We collected the papers reviewed by the above and considered this to be the initial pool of approximately 20 papers. Since our primary focus was not to present a literature review but rather to get an essence of the current solutions present, we started our search with a limited pool. From our initial pool, we selected four papers based on the following parameters: Relevance to AR, VR or MR, highly cited, recent papers (2018 +), provides a specific solution to the Bystander Privacy Problem (BPP).

The selected papers were evaluated keeping in mind the needs put forward by the survey participants and a few other parameters that evaluate the suitability for deploying it on an MR device. The parameters evaluated were:

1. Explicit or Implicit system: Definitions as mentioned above. We selected an equal number of papers (two each) in each category. Notably, the latest papers are explicit systems, with the rise of advanced computer vision and machine learning models.

2. Suitability for MR systems:
   - CPU overhead: Most popular MR systems come as HMD devices. As mobile devices, it is important to consider their resource needs, hence the CPU overhead was tagged as high, low and moderate based on the kind of model (more parameters, more compute) or time complexity when specified.
   - Algorithm performance: Any performance metric reported, such as the accuracy, specificity or sensitivity scores reported, for bystander detection.
   - Real-time processing: Can the models do inference in real-time?

3. An empirical measure of effort required by the user or bystander in operating the BP system. It is important to consider this as we do not want to increase the cognitive load in an already rich experience provided by MR systems.

4. Usability: Can the bystander privacy module affect the usability of the system?

5. Contextual clues: Was specific measures taken to hide bystanders in a public setting when they are at risk of being captured by strangers?

4 Evaluation

We evaluated two null hypotheses to validate our research questions.

Null Hypothesis 1: Users are not aware of the privacy concerns around mixed reality(MR) systems.

Null Hypothesis 2: Existing proposed systems already fully address the populace's privacy concerns around MR systems.

The data for evaluating null hypotheses come from the survey and the metrics measured during our literature review study. For each category (implicit and explicit systems), we selected two papers and evaluated the solutions using the metrics specified in section 3.2.

4.1 User Survey Results

Participant's responses were translated to a numeric value along a Likert scale of 1-5(generally lower score indicate a higher concern of MR privacy issues). The only group of questions where their scale was in reverse(higher score indicated more concern) was for the type of solution. Questions providing only four options were translated to a value between one and five with three excluded. Comparison between groups were primarily done through comparing average scores and one-way ANOVA testing. Since our goal was to test if there was a significant difference in mean (e.g: of the concern

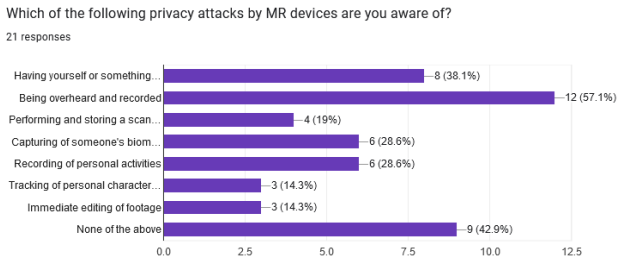

Figure 1: Survey results on awareness of privacy attack

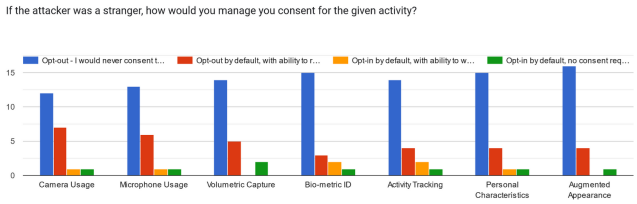

Figure 2: Consent Preferred If Stranger

scores) between any two groups and for a small sample size, one-way ANOVA testing was the most appropriate.

When measuring awareness, we counted how many types of privacy attacks participants were aware of before being presented with the scenarios. Participants were considered, "aware", if their score was greater than three.

4.1.1 Population

We ultimately collected responses from 21 participants. 85.7% of participants come from Gen Z. We only had three responses from other age groups. Most participants were male (71.4%) and 71.4% received a bachelor's degree or higher.

4.1.2 Experience with MR Devices

Participants predominantly had either experience or knowledge of virtual reality(VR) devices. Most (66.7%) had used an VR, AR, or MR device a couple times. 14.3% have no experience with any of them. Most used these devices for gaming, with one noting they used in a research study. Most participants were aware of being overheard(attacks via microphone) at 57.1%. Notably, 42.9% knew none of the presented privacy attack types.

4.1.3 Awareness

38% of participants had some awareness of privacy issues, knowing at least three types of privacy attacks in MR. 42.9% had no awareness of any presented issues. Participants were most aware of being recorded by microphone devices (57.1%). They were least aware of two attacks: personal characteristics (14.3%) and augmented appearance (14.3%).

4.1.4 Concern

Concern was measured by combining and averaging the scores for each question related to a type of attack. The average concern score was 2.25, indicating there was modern concern among participants.

We presented questions across different types of attackers. When averaging the scores between these groups, the most concerning attack was augmented appearance. However, one-way ANOVA testing gives a p-value of 0.83. Since the score is higher than 0.05, the difference in the scores are insignificant and concern is not significantly different between attack type.

We also performed one-way ANOVA testing across the different types of attackers(family v. friend v. acquaintance v. stranger). Participants were most concerned of strangers, averaging a score of 1.9. This conclusion is enforced by one-way ANOVA testing attaining a p-value of 0.0115.

When asked if they or someone else was the user of an MR device, they generally preferred implicit solutions over explicit regardless of their position in respect to the device. One-way ANOVA testing enforces this with a p-value of 0.95, demonstrating there was no difference in preference between if the user was themselves or a stranger.

Comparing the average concern score between groups on if they already knew about an attack we discover that scores had an average difference of 2.72. One-way ANOVA testing between these group's average score for each attack type attains a p-value of 0.063. Despite the small difference, this indicates that, within our population, there was no significant difference in scores if participants already knew the attack type.

Lastly, we asked a question about if they felt their concern was different between MR devices and smartphones as presented. The average answer for this question was 2.41, indicating that participants felt no difference in privacy issues between MR devices and smartphones.

4.2 Paper Analysis Results

This section presents the analysis of the solutions based on the parameters defined previously.

4.2.1 Explicit or Implicit Systems

Two implicit systems, BystandAR [6] and the solution by Hasan et al. [13], and two explicit systems, Jana et al.'s [14] privacy framework and PrivacEye [18], were evaluated. Implicit systems rely on passive methods such as eye gaze and visual cues to preserve privacy, offering seamless user experience without manual interventions. On the other hand,

explicit systems provide users with control mechanisms or visual feedback to manage privacy actively. Notably, the recent solutions, including PrivacEye and BystandAR, demonstrate the trend towards leveraging advanced machine learning and computer vision techniques for enhanced functionality.

4.2.2 Suitability for MR Systems

Both BystandAR and Jana et al.'s framework maintain low to moderate CPU overhead, demonstrating their viability for resource-constrained MR systems. BystandAR, in particular, achieves an average frame rate of 52.6 FPS when not obscuring frames and 33.6 FPS when doing so, with a 27% increase in system load. Conversely, Hasan et al.'s model is compute-intensive due to reliance on pre-trained models like ResNet50, requiring significant compression for MR device suitability. PrivacEye's CNN feature extraction bottleneck necessitates a smartphone companion device, posing challenges for MR deployment.

4.2.3 User Effort

Implicit systems, such as BystandAR and Hasan et al.'s solution, minimize user effort by automating privacy preservation processes. BystandAR leverages built-in AR features like eye gaze tracking for bystander detection, while Hasan et al.'s approach relies on visual characteristics. Explicit systems, including Jana et al.'s privacy goggles and PrivacEye, introduce user control mechanisms. While these mechanisms enhance transparency, PrivacEye's automatic shutter control eliminates manual input, though user interviews indicate a preference for some level of manual adjustment.

4.2.4 Usability

Usability impacts are minimal for BystandAR and Jana et al.'s framework, with both maintaining functionality and performance. BystandAR achieves frame rates close to the recommended 60 FPS for smooth MR experiences. In contrast, Hasan et al.'s solution, as a static analysis tool, does not impact usability directly but requires adaptation for dynamic environments. PrivacEye's reliance on a companion device and CNN bottleneck poses usability challenges for MR systems.

4.2.5 Contextual Clues

Among the evaluated solutions, only BystandAR provides contextual privacy preservation, utilizing AR user gaze and voice to differentiate intended subjects from bystanders. The other solutions rely on static or generalized approaches, which may not address nuanced scenarios like public settings with varying risks for bystanders. PrivacEye's shutter mechanism protects bystanders effectively but lacks contextual awareness.

4.2.6 Suitability for MR Devices

BystandAR and Jana et al.'s framework are the most suitable for MR devices due to their low resource demands, real-time processing, and usability focus. Hasan et al.'s model requires significant optimization for MR deployment, and PrivacEye's reliance on external devices limits its practicality without further refinement.

BystandAR emerges as the most practical and advanced solution, seamlessly integrating privacy preservation into MR experiences without compromising usability. Jana et al.'s framework offers robust privacy controls but may benefit from additional contextual enhancements. Hasan et al. and PrivacEye highlight promising approaches but require substantial adaptation for MR system compatibility.

It is important to note that while these systems process different sensors' data, they primarily protect camera-based attacks. No solution was found for other kinds of attacks on bystander privacy such as microphone usage. The solutions analyzed show that research is evolving towards the right solutions but needs improvement before it can reach the customer markets.

5 Discussion & Limitations

5.1 Discussion

5.1.1 Null Hypotheses

We expected our first null hypothesis (NH1) to be true, whereas the second one (NH2) to be false, since bystander privacy is still a new research area and would definitely have a wide range of improvements that can be done. However, after we obtained and analyzed the results from our survey, we determined that both hypotheses are false. NH1 is false because the participants are moderately aware of MR privacy issues; NH2 is also false because existing proposed systems did not address populace's privacy concerns for data related to non-camera usage.

5.1.2 Population

The make-up of the population of our survey is an important factor related to our findings. Since we previously mentioned that the majority of our participants are in Gen Z and have a bachelor's degree or higher, it revealed that they are young and well-educated, which implies that they might also be more likely to know about trending technologies, including MR devices. This eventually leads to our finding that they are moderately aware of MR privacy issues, as well as their attitude of showing concerns among different types of activities on MR devices.

Paper	Attack type	System type	CPU overhead	Accuracy	Real-time processing	Effort by user	Usability impact	Contextual clues
BystandAR	Camera	Implicit	Low	98.14%	Yes	None	Low	No
Photo	Camera	Implicit	High	93%	No	Minimal	Not usable	No
AR recognizers	Camera, Volumetric capture	Explicit	Low	86%	Yes	Minimal	Low	No
PrivacEye	Camera	Explicit	High	73%	Yes	Minimal	High	Yes

Table 1: Summary of analysed solutions

5.2 Limitations

5.2.1 Survey

Our study came under a number of limitations. We have a heavily biased and small population. Most of them are male, Gen Z, or have a bachelor's or higher. And our participants only numbered 21 individuals. Despite the p-value being higher than 0.05, it is only 0.013 larger, indicating that our scenarios introduced some level of bias. We also presented all the scenarios at once, potentially convoluting them in participant's minds. The survey's length also may have an impact on results, a pilot study participant noted their attention waned as the survey continued. Despite shortening it, it still took between 20 and 30 minutes.

Future work may be best used to address these shortcomings. A larger and more diverse population would rectify most concerns. A heavy survey redesign could fix issues on its length and ensure authenticity of responses.

5.2.2 Paper Analysis

The main limitation on our paper analysis is our small selection of solutions. This prevents us from making any wide statements about if current research trends towards implicit or explicit solutions. And while the papers are recent, a wider study across the years would provide a description if the type of solutions changed over time. Future work would hopefully focus on studying papers across a larger range of papers to interpret current trends and tendencies.

6 Conclusions

In conclusion, with the advancement and the ever-changing landscape of mixed reality (MR) devices, bystander privacy remains a crucial topic to be discussed in the field of usable security and privacy. By performing a user study in the form of a survey, we were able to gather valuable results and insights about user perceptions on this topic. Overall, participants demonstrated moderate awareness towards privacy issues in MR systems, as well as concerns in different activities, possibly due to their education level and the current trends of MR technologies.

When it comes to the implementation of solutions, we concluded that bystanders prefer implicit solutions regardless of the attack types, in which the MR device should take responsibility in safeguarding the users' privacy, contrasted to explicit ones, in which users need to take actions. Additionally, bystander are concerned about attacks from strangers, compared to people they are familiar with. Within different types of privacy concerns, there is currently no solution that addresses specifically data collected through microphones. Among the four papers we found, BystandAR [6] remains the most effective existing solution, which addresses eye movements and voice to focus on the intended. Nonetheless, we determined that the usability it addresses within stills needs to be improved. Lastly, we discovered that none of the existing solution was able to differentiate with the types of the bystander (e.g. between family members and strangers, etc.), which remains a field for future researchers to explore. In the end, we recommend future researchers to develop a comprehensive privacy framework that covers all types of privacy attacks, which would provide a better picture to tackle potential issues related to bystander privacy in MR systems from all angles.

References

[1] Apple vision pro - technical specifications. *Apple*, 2024.

[2] Agnieszka Andrychowicz-Trojanowska. Basic terminology of eye-tracking research. *Applied Linguistics Papers*, (25/2):123–132, 2018.

[3] Masaharu Ban and Ryosuke Eguchi. Vision pro teardown - japan-made parts make up 40% of new device. *Nikkei Asia*, 2024.

[4] Gabriele Bleser and Didier Stricker. Advanced tracking through efficient image processing and visual–inertial sensor fusion. *Computers Graphics*, 33(1):59–72, 2009.

[5] Yuval Boger. Overview of positional tracking technologies for virtual reality. *Road to VR*, 2014.

[6] Matthew Corbett, Brendan David-John, Jiacheng Shang, Y. Charlie Hu, and Bo Ji. Bystandar: Protecting bystander visual data in augmented reality systems. In *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services*, Mo-

biSys '23, page 370–382, New York, NY, USA, 2023. Association for Computing Machinery.

[7] Hewitt D. Crane and Carroll M. Steele. Generation-v dual-purkinje-image eyetracker. *Appl. Opt.*, 24(4):527–537, Feb 1985.

[8] Jaybie A. De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. Security and privacy approaches in mixed reality: A literature survey. 52(6), October 2019.

[9] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. In situ with bystanders of augmented reality glasses: perspectives on recording and privacy-mediating technologies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, page 2377–2386, New York, NY, USA, 2014. Association for Computing Machinery.

[10] Michael Dimock. Defining generations: Where millennials end and generation z begins, Jan 2019.

[11] Jaybie Agullo de Guzman, Aruna Seneviratne, and Kanchana Thilakarathna. Unravelling spatial privacy risks of mobile mixed reality data. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 5(1), March 2021.

[12] David Harborth and Sebastian Pape. Investigating privacy concerns related to mobile augmented reality apps – a vignette based online experiment. *Computers in Human Behavior*, 122:106833, 2021.

[13] Rakibul Hasan, David Crandall, Mario Fritz, and Apu Kapadia. Automatically detecting bystanders in photos to reduce privacy risks. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 318–335, 2020.

[14] Suman Jana, David Molnar, Alexander Moshchuk, Alan Dunn, Benjamin Livshits, Helen J. Wang, and Eyal Ofek. Enabling fine-grained permissions for augmented reality applications with recognizers. In *Proceedings of the 22nd USENIX Conference on Security*, SEC'13, page 415–430, USA, 2013. USENIX Association.

[15] Gareth Jones. Echolocation. *Current Biology*, 15(13):R484–R488, 2005.

[16] Diederick C. Niehorster, Li Li, and Markus Lappe. The accuracy and precision of position and orientation tracking in the htc vive virtual reality system for scientific research. *i-Perception*, 8(3):2041669517708205, 2017. PMID: 28567271.

[17] Joseph O'Hagan, Pejman Saeghe, Jan Gugenheimer, Daniel Medeiros, Karola Marky, Mohamed Khamis, and Mark McGill. Privacy-enhancing technology and everyday augmented reality: Understanding bystanders' varying needs for awareness and consent. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 6(4), January 2023.

[18] Julian Steil, Marion Koelle, Wilko Heuten, Susanne Boll, and Andreas Bulling. Privaceye: privacy-preserving head-mounted eye tracking using egocentric scene image and eye movement features. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications*, ETRA '19, New York, NY, USA, 2019. Association for Computing Machinery.