Speculative Privacy Concerns About AR Glasses Data Collection

Andrea Gallardo
Carnegie Mellon University
agallar2@andrew.cmu.edu

Chris Choy*
Carnegie Mellon University
cchoy2@alumni.cmu.edu

Jaideep Juneja*
Carnegie Mellon University
jjuneja2@alumni.cmu.edu

Efe Bozkir
University of Tübingen
efe.bozkir@uni-tuebingen.de

Camille Cobb
University of Illinois
camillec@illinois.edu

Lujo Bauer
Carnegie Mellon University
lbauer@cmu.edu

Lorrie Cranor
Carnegie Mellon University
lorrie@cmu.edu

ABSTRACT

As technology companies develop mass market augmented reality (AR) glasses that are increasingly sensor-laden and affordable, uses of such devices pose potential privacy and security problems. Though prior work has broadly addressed some of these problems, our work specifically addresses the potential data collection of 15 data types by AR glasses and five potential data uses. Via semi-structured interviews, we explored the attitudes and concerns of 21 current AR technology users regarding potential data collection and data use by hypothetical consumer-grade AR glasses. Participants expressed diverse concerns and suggested potential limits to AR data collection and use, evoking privacy concepts and informational norms. We discuss how participants' attitudes and reservations about data collection and use, like definitions of privacy, are varying and context-dependent, and make recommendations for designers and policy makers, including customizable and multidimensional privacy solutions.

KEYWORDS

privacy, augmented reality, data collection, contextual integrity

1 INTRODUCTION

Augmented reality (AR) glasses pose privacy concerns, with their potential to collect sensitive user data—such as biometrics (heart rate, eye tracking, voiceprint) and bystander face images—and to combine such data to infer even more sensitive user or bystander characteristics, such as health status. The failure of Google Glass, Google's AR glasses, a decade ago is sometimes attributed to a lack of consideration for societal norms and privacy expectations [22, 38]. As information norms for consumer-grade AR devices are still being established, a better understanding of context-relevant privacy risks and concerns can help inform the design of these technologies and help ensure that they respect privacy.

We explore potential privacy and security concerns regarding AR glasses data collection through 21 semi-structured interviews with current users of AR technologies available to general consumers. We told participants to imagine they had a more advanced (hypothetical) pair of AR glasses and asked them how comfortable they would be with the collection of 15 types of data and five data use cases. Our research questions were as follows: (RQ1) What are participants' attitudes and concerns regarding data collection and use by future AR glasses? (RQ2) Which data actors and data subjects are participants concerned about? (RQ3) What privacy principles do they expect or hope for?

We used qualitative coding methods to analyze the interview data, using a priori attitude labels and also iteratively developing emergent codes. Most participants were uncomfortable or had mixed feelings about certain data types, such as face images, brain waves, and voiceprints. They also had concerns regarding potential data actors, such as data collectors or receivers (e.g., employers, advertisers, and doctors) and data subjects, such as bystanders or their children. Participants also presented potential context-relevant privacy harms as well as potential harms to people in vulnerable situations or groups. Privacy principles desired by participants included control over data collection and use, providing notice, requiring consent, collecting or using only necessary information, and protecting sensitive information.

Our exploratory study provides insight into current AR technology users' privacy concerns regarding data collection by future AR glasses and their desired privacy principles. From these insights we offer recommendations for AR professionals and lawmakers.

2 BACKGROUND AND RELATED WORK

Below we discuss AR glasses technology, including current and future data collection capabilities, as well as prior work on privacy and security concerns about AR, mixed reality (MR), and virtual reality (VR) glasses, and related technologies. We outline some privacy concepts or frameworks, which we use to analyze participants' responses in our study, and prior work on privacy risks for people in vulnerable situations or groups in VR and online contexts.

2.1 Background on AR Glasses

Augmented reality (AR) is a technology that augments a user's visual and audio perception of reality with interactive virtual overlays.

*Most of this work was completed while the authors were at Carnegie Mellon University.

Proceedings on Privacy Enhancing Technologies 2023(4), 416–435

https://doi.org/10.56553/popets-2023-0117

AR glasses are wearable head mounted display devices that provide such functionalities and are different from other devices that use sensors, such as mobile phones or IoT devices, in their distinctive combination of form factor, functionalities, and sensors. They are sometimes also considered mixed reality (MR) glasses, when they provide the ability to interact with both virtual and physical objects, in contrast to VR glasses, which provide fully virtual interactions.

2.1.1 Information Flows for AR/MR/VR Glasses and IoT. We discuss types of data collected and used by AR and MR glasses, as well as by wearable IoT technology, such as smart watches, whose sensors and features may be integrated into AR devices in the future. These helped determine the data types and data uses we asked our participants to consider. Data collected by these devices' sensors often contain personal or sensitive information, or could be combined with other data types to reveal such information. We also anticipate AR glasses integrating mobile device features like notifications, face filters, and location mapping, as some mobile AR apps or features utilize cameras, e.g., to overlay digital graphics on camera images, allowing people to create or adopt face filters, or use location mapping, e.g, for mobile AR gameplay in Pokémon GO.

AR Glasses Sensors and Features. The number of sensors in AR devices has increased, but as prior work notes, not all components are made known by companies and sensor presence sometimes has to be "inferred from device functionality" or "direct observation by taking it apart or consulting online resources detailing such observation" [61]. Recent mass market AR glasses are equipped with basic sensors, such as microphones, speakers, or cameras, to collect audio and video or image data and to detect surroundings, but have limited (or sometimes no) embedded displays, with overlain images sometimes serving primarily to display video or browser content rather than content that interacts with one's environment [35, 87], Realistic AR integration of overlain objects and visual perception of physical surroundings has not yet been achieved.

Enterprise level AR glasses tend to have additional sensors, cameras, and tools to track a user's eye and body movement, map surroundings (such as indoor spaces), and create 3D models. The HoloLens2 sensors include visible light and infrared cameras, a depth sensor, an inertial measurement unit (IMU), and a camera capable of recording video. It also collects biometric data such as eye tracking and body movement data [8, 71]. In addition to similar sensors, Varjo's XR-3 headset uses light detection and ranging (LiDAR) for depth-sensing [95]. The way that data is stored also varies between devices, e.g., Hololens2 eye-tracking data is stored as eye gaze vectors [72], while Varjo's eye tracking data consists of "foveated rendering" and raw video recordings of eye movement [103]. Apple's yet-to-be-released Vision Pro glasses use 12 cameras, five sensors, and six microphones, including "high-speed cameras and a ring of LEDs" for eye tracking [5].

IoT sensors and features. We anticipate AR glasses integrating features of wearable IoT devices like fitness trackers and smart watches, which can collect biometric data such as heart rate, body temperature, and movement data, and are used for health monitoring [97]. We also imagined AR glasses containing sensors or features not yet generally marketed to consumers, such as brain wave data collected by EEG sensors (currently integrated into MR glasses as part of Varjo's Galea Beta Program) [31, 32, 48, 96, 106], facial recognition [47, 53], the capture and use of voiceprints [26, 57, 99, 110] and reaction times [89], and feedback about facial expressions [64, 73, 91], mood [29], or social interactions [109].

2.1.2 Privacy Policies for Current AR/VR Glasses. Current privacy policies vary in the amount of detail they provide about AR or VR glasses data collection and contain little to no detail about inferences made using headset data. For example, Google's, HTC Vive's, and Varjo's devices' Terms of Service agreements direct readers to their companies' general privacy policies, which do not mention how device data is used [14, 15, 28, 30, 104, 105]. Meta provides various privacy notices, some specifically addressing data about movement and recording in virtual worlds [67–70]. In immersive VR settings, the Oculus collects audio recordings "through a rolling buffer processed locally on-device" that can be stored on Meta's servers if a report is submitted to them to report abuse or harmful conduct [68]. Apple provides a general privacy policy as well as "product-specific" policies for features that exist across different Apple devices [4, 6]. Apple Vision Pro promotional materials also state sharing limitations for information about a user's iris, eye tracking information, and data from the camera and other sensors [5].

Yet, as has been observed in prior work [1], no full accounting of data collection practices is provided in these legal notices. Meta and HTC also inform users that separate privacy conditions apply for services or products provided by third parties [14, 15, 69]. Magic Leap and Snap, unlike Google, HTC Vive, or Varjo, provide more detailed privacy policies for their glasses, covering what information is collected, how it is used, and with whom it is shared [41, 43]. While their devices have different types of sensors, e.g., Magic Leap 2 can track users' eyes [42], whereas Snap Spectacles 3 cannot [44], both privacy policies clearly state the data collected from different sensing modalities and, like Meta and Microsoft, mention general uses for collected data: personalizing content, improving user experience, and product development. However, whether and what inferences are made about users with the collected biometric data (e.g., eye tracking, audio) is not stated and remains vague.

2.2 Privacy and Security Concerns

In this section, we discuss prior work that addresses user concerns about AR glasses and related technologies. Prior work has anticipated potential privacy and security harms arising from AR glasses [12, 55, 88] and AR applications such as mobile AR games [84]. De Guzman et al. outline potential mixed reality privacy and security risks and provide a survey of prior work addressing them [17]. Harborth et al. showed a gap between users' understanding of threat models and actual privacy and security risks of certain mobile AR permissions, such as accelerometer data, which tracks movement [33]. Prior work has also considered potential privacy and security risks of data inference, which users may be unaware of. Cong et al. designed an eavesdropping attack using zero-permission motion sensors in AR/VR glasses to infer speaker gender, identity, and speech content from live human speech [92]. Bye et al. raised concerns that biometric data could be used to infer an MR glasses user's membership in marginalized groups, noting that gaze data can reveal users' sexual preferences [12, 85]. Other work confirms

that eye tracking can reveal gender, sexual preference, age, race, affect, emotional state, health, and task focus [52, 59, 108].

Yet, only a few studies have considered current or potential AR glasses users' privacy and security concerns [18, 33, 50, 51, 55, 86]. These explored participants' general feelings of comfort, acceptability, or concern about unspecified general AR or MR glasses usage, but our study is the first to focus on current AR users' concerns about AR glasses collecting and using specific data types.

2.2.1 AR technology. In prior work surveying or interviewing end users or potential users of AR technology, participants' privacy and security concerns include AR glasses capturing private information, collecting data about their physical surroundings, biometrics and private activities, bystanders' privacy and security, risks posed by overlain content, and security compromise of AR devices or apps [18, 55, 78]. Koelle et al. conducted two studies gauging acceptability of the general use of "data glasses" and found that social context, such as whether other people were present, was a factor in how acceptable participants found the glasses [50, 51]. Denning et al. found that bystanders in an AR context were concerned about being identified, citing reasons like bodily harm as imagined negative consequences [18]. Rixen et al. addressed potential users' comfort with AR technology displaying personal information (rather than with data collection or use, as in our study), and found that factors such as people present ("intimacy") and whether information was self-disclosed or not influenced participants' comfort level [86]. A survey conducted by O'Hagan et al. showed that participants' privacy wishes and preferences, as hypothetical bystanders to AR glasses' sensing and data collection, varied by feature and was also context dependent, with participants providing examples of situations they would find problematic [78].

2.2.2 Social VR and Online Social Contexts. Prior work has considered privacy and security concerns in the contexts of social VR (VR communities that allow live interaction between users, such as VR Chat, AltspaceVR, or Horizon Worlds) and online communities in which the use of pseudonyms and avatars can protect anonymity and allow users to engage in selective self-disclosure. Studies on self-disclosure in social VR show that while some users expressed feeling more comfortable sharing personal information about emotions, sexuality, lifestyle, and personal goals when using anonymous avatars than in person, many had concerns about disclosing personal information about gender, cultural or linguistic background, or disability status through their voices, avatars' features, or behavioral patterns [62, 98, 111]. On social media, Li et al. found significant differences in female and male privacy disclosures [58], and Pyle et al. shed light on how a user's LGBTQ identity might lead them to not disclose potentially stigmatizing information such as pregnancy loss [82]. Prior work has also noted the potential for VR to both reinforce and mitigate social prejudice [101].

However, users, especially those from non-dominant groups, face privacy and security risks that may discourage participation [25]. Prior work has shown that online harassment or suppression of marginalized community members by dominant group members has occurred in online gaming communities such as Second Life and Massively Multiplayer Online Role-Playing Games [10, 16, 24, 66, 100], as well as on social media [77, 102]. VR and AR technologies allow for more immersive interactions, e.g., the ability to simulate physical interaction and intimacy, which has also led to simulations of sexual harrassment and assault [62, 92]. Some scholars have also suggested that norms based on a majority or dominant group's practices may result in exclusion and increased marginalization of people who cannot or do not conform to these existing norms [65]. In a study on VR in the context of disability, Gerling et al. argue that the design of VR technology assumes a normative "corporeal standard" and consequently excludes disabled people by failing to adequately accommodate them [27]. In our study, participants identified similar possibilities for exclusion, harm or discrimination.

2.2.3 IoT and Wearable Cameras and Recording. Prior work in the context of IoT has explored concerns related to wearable cameras, such as lifelogging cameras [39, 40, 80], as well as photo and video recording in public [81], and private [39] spaces. People have also expressed concerns about bystander privacy being violated by cameras [23, 40, 81]. Considering that the frame rates of traditional AR head-mounted displays are likely higher than some of these lifelogging cameras [40], more fine-grained data collection and possible combinations of data for inference may pose privacy issues.

2.3 Attitudes and Comfort Levels

Prior work capturing user attitudes towards privacy has used comfort as a proxy for how participants feel about a given topic [36, 46, 60], including AR [34, 54, 86]. Some of this work [34] focused on developing scales that measure how much benefits of using AR outweigh privacy concerns or vice versa. In contrast, our study uses qualitative methods to elicit more and richer detail than such scales could capture about potential privacy concerns, through the lens of participants' feelings of comfort or acceptability and discomfort or non-acceptability of AR glasses data collection or use.

2.4 Privacy Concepts

Here, we note various concepts of privacy, which we will apply to participants' responses about data collection and use, in Section 7. We also note some shortcomings of these concepts.

Some common conceptions of privacy include privacy as seclusion (freedom from intrusion), control over personal information (ability to control information flows), and confidentiality (preventing unwanted disclosure or exposure) [3, 37, 90]. Scholars have suggested that there are private spheres and public spheres, distinct spaces or contexts delineating privacy boundaries [74]. Yet, there is no single definition of privacy, and critics of such privacy concepts point out that they are not able to capture the diversity and complexity of privacy across contexts and societies [3, 37, 76, 93]. Hartzog writes, "When lawmakers and judges accept privacy as a concept that contains multitudes, each of these different notions can explicitly be brought to bear on the real needs of people, groups, and institutions rather than deploying an ill-fitting theory in diverse contexts" [37]. For example, privacy as control has inspired frameworks such as notice and choice, but such "privacy self-management" approaches make individuals responsible for protecting themselves even in the face of overwhelming amounts of privacy policies or insurmountable imbalances of power [37, 94].

Nissenbaum and Solove have proposed frameworks for considering the practical implications of privacy violations. Solove's work considers privacy problems and harms using a taxonomy with four

categories of problems, i.e., "four basic groups of harmful activities": (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion. Each of these groups consists of different related subgroups of harmful activities. In this study, we apply a subset of Solove's taxonomy of privacy harms to the privacy concerns voiced by participants [93]. These include the subgroups of aggregation, appropriation, breach of confidentiality, disclosure, distortion, exclusion, exposure, identification, intrusion, secondary use, and surveillance. Prior work has mapped Solove's taxonomy to participant concerns in interview studies, focusing on connecting them to the taxonomy's four categories of problems [2, 9, 13]. While our work focuses on concerns about data collection, participants also brought up concerns spanning these four categories.

Nissenbaum's norms-based approach to privacy, known as contextual integrity, is concerned with "context-relative informational norms," which are social norms "specifically concerned with the flow of personal information." Contextual integrity requires that "practices affecting information flows be assessed in terms of their compliance with context-relevant information norms," which can be evaluated in terms of "values, purposes, and goals." She suggests that informational norms that regulate social behavior (e.g., acceptable actions or practices) in contexts of social life should also exist in digital contexts, and that these norms should be discussed and established by all stakeholders, rather than having arbitrary rules stated by companies [74–76]. Scholars have used Nissenbaum's Contextual Integrity framework to investigate whether privacy attitudes or expectations align with existing data flows. Apthorpe et al. used surveys to study how participants' attitudes aligned with data regulations [7]. Zhang et al.'s qualitative analysis of survey responses revealed that nuanced ethical and social values informed participants' "normative assessment of the perceived appropriateness of" a given technology [112]. Participants in our study often raised context-relative privacy considerations and emphasized contextual factors, such as physical location, social context, or data actors involved in the information flows. We discuss potential connections to contextual integrity in Section 7.2.

3 METHODS

Our study consisted of 21 semi-structured interviews with current AR technology users and was approved by our institution's IRB. We describe recruitment, interview, and data analysis methods below.

3.1 Recruitment

We recruited participants with varied prior AR experiences through posts to Reddit forums and an email listserv related to new media (e.g., AR), seeking permission from forum moderators to post our recruitment text (Appendix A). Specifically, we recruited from forums for general AR or Hololens users (r/hololens, r/augmentedreality) and forums for fans of mobile AR games Ingress, Pokémon GO, and Harry Potter Wizards Unite (r/ingress, r/pokemongo, r/hpwu). The breakdown of recruitment sources by participant is included in Appendix D. We paid participants $20 for 60-minute interviews and $30 for 90-minute interviews.

We asked all potential participants to fill out a screening survey to ensure they spoke and understood English, were located in the U.S. were at least 18 years old, were able to install and run Zoom for the interview, and had used at least one AR app or device recently. We purposefully invited participants of various gender, racial, and ethnic identities from among those who filled out the screening survey to participate in the study. We anticipated that users with prior experience using current AR technology would be more knowledgeable about what data can be collected and more aware of possible privacy and security risks than other people, and might also have insights about using AR devices that travel with them and collect data in varied social contexts (e.g., work, education).

Data Types		
Audio	Video or Image	Location
Indoor Spaces	Virtual Spaces	Heart Rate
Body Temperature	Brain Waves	Movement
Eye Tracking	Face Images	Expressions
User Voiceprint	Bystander Voiceprint	Reaction Times
Data Uses		
Notifications - reminders or notices alerting the user		
Health Monitoring - health feedback based on biometric data		
Social Feedback - based on interaction data, gesture or voice		
Face Filter - overlain images used as avatars or accessories		
Mood/Emotions - predicted emotional state (e.g, based on tone)		

Table 1: 15 Data types and five data uses collected or used by hypothetical AR glasses.

3.2 Interviews

Using an interview format (21 semi-structured interviews) instead of a survey allowed us to elicit participant responses that better captured nuances, conditionals, and mixed or conflicted opinions. We piloted the study with five participants and then revised the protocol substantially to focus our questions more on data collection. We piloted the revised study with two additional participants, who completed it in under 60 minutes.

Each interview took place over Zoom and was recorded and automatically transcribed after obtaining consent to record. Only one participant chose to leave their video on during the recording. The first 11 interviews took up to 60 minutes, and the last 10 interviews took between 60–90 minutes. We extended the interview length, as we were often unable to complete it in 60 minutes.

The interviews started with questions regarding background information on prior AR technology use and participants' understanding of data collection practices of the AR technology they most often use. The main part of the study consisted of questions regarding participants' attitudes toward data collection and use by hypothetical AR glasses. We asked participants whether they would be comfortable or uncomfortable with the collection of 15 specific data types and five specific data uses (listed in Table 1). For the data use of health monitoring, we also asked whether they would be willing to share this data with doctors, researchers, or fitness apps. We also asked two yes-or-no questions about facial recognition (related to the data type of Face Images), i.e., whether they would use this feature and whether they would allow it to be used on them. The data types we asked about are based on current and anticipated AR and VR glasses data collection features (see

support in Sections 2.1 and 2.2.2). While these cover a broad range of possibilities, they were not exhaustive and were kept general enough to be understandable, to avoid distracting or confusing participants with specific details about sensors or cameras, which may also change over time. These questions allowed participants to envision use cases before being prompted with benefits, harms, or questions about data use, which elicited thoughts about possible applications of data types.

If a participant expressed clear comfort or discomfort with the collection or use of a particular type of data, we prompted participants with a pre-written example use case of a benefit or a downside, whichever contrasted with their initial opinion, and we kept track of whether they modified their response to the opposite comfort attitude based on our prompt or maintained their initial stance. After neutral or unfamiliar responses, we provided examples of both benefits and harms. Benefit and harm examples encouraged participants to consider attitudes contrasting with their primary attitude, intentionally probing whether examples could influence their opinion, rather than relying on existing knowledge (or unfamiliarity). In response, participants generally provided conditions for maintaining their original stance or acknowledged the benefit or harm but did not change their overall attitude. For the four instances where participants changed their attitude, we report only the final attitude in our summary of participant attitudes.

We did not prompt participants to discuss privacy concerns and avoided the word "privacy" in our questions, focusing instead on obtaining participants' concerns specific to data collection and use.

We ended the interview with 11 general questions (GQ) about whether certain aspects of AR glasses data collection or data use would make a difference to participants. These aspects included location (GQ1), time of day (GQ2), certain social contexts (GQ3), data subjects (GQ4), data collectors and receivers (GQ5), data storage (GQ6–7), deletion options (GQ8), data transfer options (GQ9), and data collection notifications (GQ10–11). The structured parts of the interview script are included as Appendix B.

3.3 Data Analysis

We used a mix of a priori and emergent coding to code the responses to the 23 questions about data collection and use. We referred to the audio as needed to disambiguate the text and gain insight through prosody, tone, etc. After the interviews, we segmented the interview transcripts into sections, focusing on 23 questions about data collection and use.

Emergent coding. Three researchers constructed emergent codes based on their memory of participants' responses, themes in the interviews, as well as codes that would help us label general attitudes: stated positions such as Would Use/Would Not Use and Existence Okay/Existence Not Okay, and Conditional for stated conditions (e.g., "only if I consent to it"). Two researchers then used this initial list to each code two distinct transcripts and refine the codes. These two coders then double-coded all of the interviews using agreed-upon refined emergent codes, splitting the work: each coder was the primary coder for one set of interviews, responsible for coding a set of assigned interview segments, while the other coder was the secondary coder, responsible for reviewing the emergent codes and adding new ones based on their review of the same interview segments. Disagreements, added codes, and code definitions were resolved and clarified through discussion. While we believe that these codes sufficiently capture the major themes we observed in our interviews, we also note that they were the researchers' interpretations of connections between the transcripts and our research questions and that other researchers might generate a different list.

Coding of attitudes. To capture participants' attitudes toward AR glasses data collection, we labeled each question's responses with one of three codes: "Comfortable/Support," "Uncomfortable/Oppose," or "Mixed/Conflicted," first assigning the coding of one interview to two researchers. We calculated inter-rater reliability using Cohen's Kappa, which was 0.72, which we considered acceptable to proceed. In addition, we discussed and resolved all disagreements and refined what criteria were used to assign labels for each of the three attitude codes, proceeding without further double coding. We used the refined criteria to separately code the rest of the 20 interviews, with one coder coding 17 interviews and another coding three.

3.4 Limitations

Our sample of participants is small and not representative of the general U.S. population, Our study purposely selected current users of AR technology, who may have been more comfortable than other people with potential data collection by AR glasses. Thirteen participants used location-based AR games, which may have influenced how comfortable they were with location and image data collection.

We asked interview questions in the same order for every interview, which may have led to an ordering effect. For example, we noticed that some participants' emotional intensity dropped off later in the interview; later replies were more often direct and succinct, such as, "same" or "like I said before."

3.5 Participant Demographics and Prior AR Experience

Full participant demographics are shown in Appendix D. While diverse in terms of gender (10 male, 6 female, two nonbinary, one trans man, one with multiple gender identities, and one who preferred not to respond), most participants identified as white and were under 35 years old. Of the 18 participants who provided income information, eight reported making over $100,000 per year, and four reported making under $30,000. Thirteen of our participants were recruited from Reddit AR mobile gaming communities, seven from other Reddit AR communities, and one from an email listserv (see Section 3). Current AR technologies used most often by participants were mobile AR games (n=12), Hololens (n=6), and other AR mobile apps or features (n=3).

4 RESULTS: ATTITUDES AND CONCERNS (RQ1)

We first discuss participants' overall attitudes toward current AR technology and future AR glasses data collection and data use (Section 4.1). We then discuss participants' concerns about future AR glasses data flows. Some concerns specifically addressed data types from our study questions (Section 4.2), while others focused on private spheres, e.g., the home or romantic relationships (Section 4.3).

Throughout the paper, we use the terminology in Figure 1 (from Emami et al.) to refer to number or percent of participants [21].

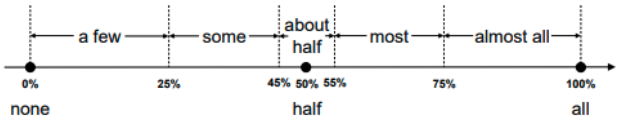

Figure 1: The terminology we use to report percentage of participants.

4.1 Overview

As described in Section 3, we asked participants how comfortable they were with current AR technology they used and how comfortable they would be with the collection of 15 data types and five data uses by hypothetical AR glasses. We coded these responses as Comfortable/Support, Mixed/Conflicted, or Uncomfortable/Oppose. Only one participant was uncomfortable with data collection by their current AR device or apps; they said they understood that the data was "very valuable and useful" from a developer and marketing perspective, but that they found it invasive as a user. Some participants were comfortable (n=8) and about half had conflicted feelings (n=11) about data collection by their current AR device or app. One participant's current AR technology was collecting data about others, so we did not ask them this question.

When we asked about future AR glasses, over half of participants, as shown in Figure 2, were comfortable with the collection of five data types and with three data uses, and were uncomfortable with or conflicted about ten data types and two data uses. Participants' attitudes ranged considerably: almost all participants (n=17) were comfortable with location data collection, and fewer than three were comfortable with the collection of face images and bystanders' voiceprints. We present specific concerns about certain data types and uses in Section 4.2.

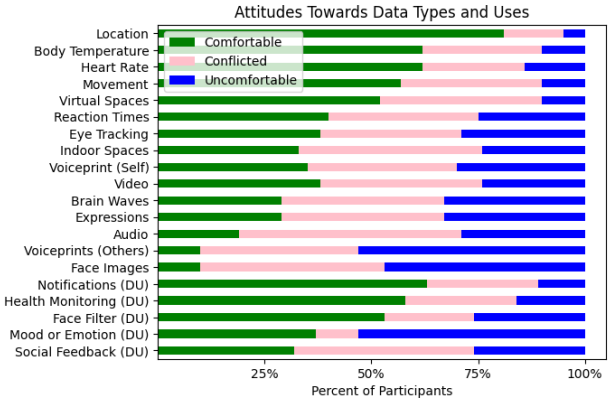

Figure 2: Number of participants expressing given attitudes (comfortable, mixed, uncomfortable) regarding the collection of each data type or data use (DU).

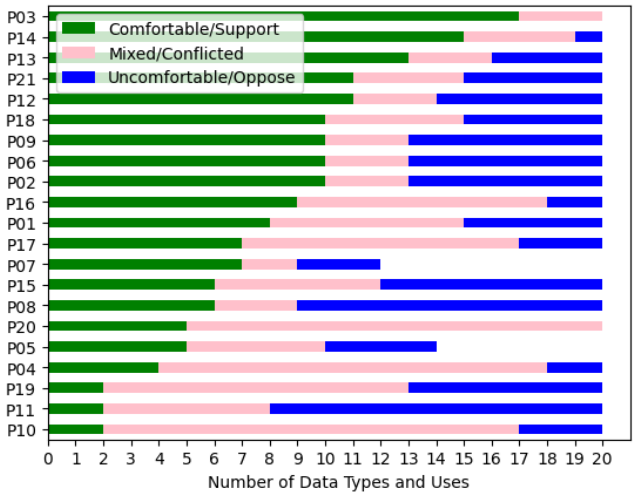

Figure 3: Participants' attitudes (comfortable, mixed, uncomfortable) regarding 15 data types and 5 data uses. Note that for some data types, counts do not add up to 20 because we did not ask some questions due to lack of time.

Examining these attitudes by participant, we find that 13 participants mostly expressed Comfort/Support, while five showed primarily mixed sentiments (Mixed/Conflicted), and three expressed mostly discomfort (Uncomfortable/Oppose), as shown in Figure 3. Almost all participants expressed mixed feelings or discomfort regarding at least nine data types or uses, and all participants expressed either mixed feelings or discomfort in responses for at least three data types or uses (types and uses varied by participant). There were only four instances of participants modifying their comfort-levels, regarding four different data types.

Our coded emergent themes capture recurring concerns and sentiments that shed light on what participants considered to be boundaries, limits, or norms for data collection and use. Fourteen or more participants mentioned the following eight concerns: Recording, Bystanders, Data Use/Purpose, Consent/Opt-in-out, Storage Matters, Context/Situation Matters, Data Protection, and Advertising. Among these, the most frequently mentioned were: Data Use/Purpose, Consent/Opt-in-out, and Storage Matters, being mentioned a total of 71, 63, and 47 times, respectively. All codes and definitions are included in Appendix C.

4.2 Data Types

Participants' attitudes towards data collection varied across data types, with no participant uniformly comfortable or uncomfortable with the collection of all of them. Some participants noted that they were already used to the collection of certain data types, such as location data (n=10) or heart rate data (n=7), for example by mobile phones or fitness trackers. Audio and video data, though used in common technologies like mobile phones and tablets, inspired discomfort based on factors such as recording and storage. We highlight here some data types about which most participants expressed discomfort or conflicted attitudes: Face Images (n=19), Audio (n=17), Video (n=13), Facial Expressions (n=15), Brain Waves

(n=15), Mood or Emotions (n=12), Eye Tracking (n=13), Voiceprint (user: n=13; bystander:n=17), and Reaction Times (n=12).

4.2.1 Face Images. Most participants objected to AR glasses using face images for facial recognition on faces detected by the glasses. P8 considered displaying bystanders' personal information (upon recognition) to be "too personal" and unnecessary. P16 said they wouldn't want their face to be "mapped" or photographed and "uploaded to wherever." P5 and P6 suggested that using AR glasses for tasks like processing faces and expressions could cause a decline in natural human abilities:

> *At that point, technology sort of crosses a line where if it's doing a lot of the human interaction for you, I feel like that's something that it's only going to lead to a dark tunnel for us, human nature wise. (P6, Face Images)*

P8 suggested facial recognition would be extraneous, saying, "I don't need the device to tell me if I recognize a person."

Audio and Video. Participants opposed to audio recording (n=14) or video recording (n=10) were sometimes concerned with AR glasses potentially collecting audio data or recordings of private conversations. P15 showed concern for users whose sensitive conversations could cause them to be "tied back to someone," which could have "legal ramifications for them, social ramifications" (Audio). P4 said they worried about potential harm resulting from someone else possessing audio recordings of them, asking, "What will someone else do about them, to me?" Some participants shared concerns about always-on recording, even if they did not consider their given action or location at the moment of recording to be private per se. P13 gave an example of a prior incident with AR glasses (Snap Spectacles) in which their friends were concerned about being recorded:

> *When I'm trying to wear those glasses and, you know just going to a beach and trying to record something like, my friends will literally get nervous, like, "Hey, are you actually trying to record me?" (P13, Video)*

P7 said they "would feel uncomfortable with any video or photo recording that was not something [they] had specifically pressed a button" to record, conveying a preference to opt-in every time.

4.2.2 Facial Expressions and Mood. Concerns about facial expression data included self-consciousness, involuntary disclosure, and being forced to consider how they present. While some participants suggested that feedback from AR glasses could help them reduce social anxiety, others said it could make them overly self-conscious if their facial expressions "were interpreted as something other than what [they] perceive them to be them about" (P9). P4 said they wanted the "privacy" of "not telling" or disclosing thoughts:

> *Maybe I'm thinking something but don't want to communicate it outwardly, but my face shows it. So when can I have that privacy of not telling someone I'm making a 'That's disgusting, why did you say that?' face [when] I'm saying, 'Oh yeah, that's awesome, thanks for sharing!' out loud. (P4, Facial Expressions)*

While some participants expressed enthusiasm about mood or emotion data helping manage anger or other emotions, about half had concerns. P9 was concerned with becoming "hyper-aware" and "overthinking." A few saw it as unnecessary and overreaching, or said it might exacerbate negative feelings.

> *No one likes to be told, "Stop being angry," and I can see where that might cause escalation. (P4, Mood or Emotions)*

While P6 liked the idea of a mood sensor, they wanted it to be an "indicator" of what they were currently feeling rather than something that "guides you to do something else." Three participants (P14, P10 and P8) considered mood or emotion information to be mental health data, and P14 called for it to be "protected under HIPAA." P8 did not think AR glasses should be tasked with mood evaluation, saying, "It should be best to have a doctor evaluate you for any mood issues."

4.2.3 Brain Waves. While some participants acknowledged potential health benefits of brain wave data collection, most expressed concerns. P17 said it would be inappropriate for consumer devices:

> *There's no reason for that to be in a regular consumer headset. I think that's just outside of the scope of what people buy these things for. (P17, Brain Waves)*

A few suspected harms or invasive applications, with P12 saying that "it feels a little bit like mind reading," and that they "don't want anybody knowing [their] internal state." P7 noted that "brains are incredibly complicated" and suggested that "it's very easy for data to be misused" or misinterpreted, e.g., through "workplace wellness programs." P19 suspected that brain wave data could be used "to track people with some kind of log that can identify your personal brain" based on patterns. P15 suggested it could help create an "advertising monster" to "get [them] to buy more [things]":

> *I wouldn't want, based on what readings are being taken from my brain, [to] then have correlating visual material presented: "Hey we noticed you're depressed all the time, based on your brainwaves here. Try to talk to your doctor about this drug." You know, that's where I get really afraid, is like the advertising monster that AR can enable. (P15, Brain Waves)*

A few participants said they would like to have more information before deciding to use the feature. P18 felt its strangeness or novelty warranted an official company explanation, given the "implicit power in that data and personalized nature of it."

4.2.4 Eye Tracking. While most participants had concerns about eye tracking data collection, a few participants thought it would be necessary for the glasses to function or were resigned to it, noting it was already happening in retail stores (P6). P12 said they would be uncomfortable with eye tracking data being combined with video data in the home. P2 suggested that eye tracking data linked to past experiences could "be negative" because it may evoke "bad experiences" and exacerbate anxiety-related ruminations. P13 preferred that AR glasses not collect recordings for eye tracking data, but rather processed data, e.g., eye gaze vectors.

Some participants expressed concerns about eye tracking data being used for advertising and a few said they did not want ads to fill or obstruct their view. P21 hoped for restrictions or ad blocking features, for example on "when and where" ads could appear, or

legal restrictions "on what developers and companies that build applications are allowed to do in terms of advertisements."

4.2.5 Voiceprints (User and Bystanders). Participants' concerns about voiceprints (distinctive patterns based on a person's voice that can be used to identify, authenticate, or impersonate that person) included storage, bystanders, and impersonation. P20 was concerned about biometric data being leaked if not stored securely and preferred that voiceprints only be used for authentication. P15 suggested having a local voice profile to lock the device and prevent unauthorized users from issuing voice commands:

> *I would be okay with them . . . collecting enough data to build a local profile on the device where it can decipher my voice from everyone else . . . so someone can't do what people did with Google glass—run up and say, Hey Google, search blah blah blah . . . and open it in 100 tabs. (P15, User Voiceprint)*

P19 considered voiceprint data collection to be "more about access to your microphone," suggesting that any audio data collection could potentially capture voiceprints. P10 suggested that recording laws should apply to voiceprint data. Some (n=8) participants expressed concerns about bystanders (see also Section 5.2). P16 suggested having a "guest mode" or "visitor mode" to remove personalized analysis of bystanders' voice patterns. A few participants were also concerned about impersonations or "deep fakes," and suggested imposters could use voiceprints to demand money from family members, falsely authenticate, produce a fake conversation they never had, and use voices for advertising.

4.2.6 Reaction Times. Three participants suggested that reaction times could reveal health changes, such as worsening conditions, but they felt differently about this possibility: while P18 found it helpful, P20 said they weren't sure, and P2 said they would not want this data to be revealed or shared by the AR glasses. Most participants were especially uncomfortable with reaction time data being collected by insurance companies after we gave an example of them increasing premiums after observing slow reaction times on breaking, with P3 saying, "Even the best of drivers would never agree to something like that." P16 noted that reaction time data could already be collected by car insurance telematics systems.

4.3 Private Spheres

Participants expressed concerns about data being collected in certain locations or social situations, like activities and relationships.

4.3.1 Private Places or Physical Locations. Specifying spaces where they would want to limit or disable data collection, about half of participants (n=12) mentioned the home, five mentioned the workplace or office (see Section 6.4), and a few mentioned the following: doctor's office, car, government facilities, funeral places, LGBTQ+ meetings, political meetings, restaurants, church, and parties.

Home. A few participants discussed their privacy concerns about the home. P12 consistently had mixed feelings about sharing data, depending on whether they were in public or at home:

> *Within the home, it's kind of like a sacred place where you can be weird and goofy, . . . and nobody should be able to see that but you. (P12, Video)*

A few participants focused on specific rooms or activities within the home. P5 did not want AR glasses collecting video data when in the shower or on the toilet, or when "engaged in intimate actions with [their] partner." P18 felt uncomfortable with the idea of AR Glasses sending reminder notifications to clean the toilet. P13 said they would rather take their glasses off while in the home, given all the information that could be collected about them and their child. P4, P5, and P13 expressed concerns about security risks of AR glasses collecting maps of indoor spaces, e.g., burglars, with P4 suggesting the data could disclose where users keep valuables or where their children sleep.

Privacy in Virtual Spaces. Most participants (n=13) expressed discomfort or mixed feelings about data collection in virtual spaces, and three (P7, P13, P21) had concerns about potential identity disclosure, suggesting that virtual spaces allow a freedom of behavior or interaction that might be infringed upon if identities were revealed.

> *Some people, they . . . completely become like another different person when entering a game world, so they can be free for themselves, they may go out of boundary a little bit. (P13, Virtual Spaces)*

If such people were being "tracked," P13 suggested, they might not feel as free. P7 mentioned the risk of malicious actors identifying and targeting members of identity-based virtual spaces, for example, in a social VR space that "caters to trans people."

4.3.2 Private Activities and Relationships. Some concerns were not about spaces but rather activities or relationships, such as recording, family relationships, and romantic relationships.

Family Relationships. Some participants placed limits or expressed discomfort regarding data collected about their family, such as conversations within the home with family, or where children sleep, as noted above. P14 considered how lie detection using facial expression data might influence parent-child power dynamics:

> *Could you imagine how powerful parents could be if they could facially detect their children when they're lying to them? (P14, Facial Expressions)*

Romantic Relationships. Some participants noted concerns relating to romantic situations, such as dating or intimacy. P16 gave an example regarding disclosure of personal information on a date:

> *I don't want the Black Mirror episode where a couple is going on a date and the dude is getting all her information just by looking at her. That's creepy land. (P16, Face Images)*

Two participants (P4, P5) expressed not wanting the glasses to collect data while they were engaged in physical intimacy. P4 specified a time span that should be off-limits:

> *Not to be crass, but I don't want it to have it from these hours, where I know I was having sex or something, . . . unless it has some benefit, because I [would] know I'm having like a heart issue, and they need to see it during high activity. (P4 Health Monitoring)*

5 RESULTS: DATA ACTORS AND SUBJECTS (RQ2)

Participants expressed concerns about data collectors, receivers, and subjects (Sections 5.1–5.2), as well as concerns about potential harms to people in vulnerable situations or populations (Section 5.3).

5.1 Data Collectors and Receivers

Most participants (n=16) expressed reservations about data collectors and receivers, and all 13 participants who were asked whether they would like to know who or what companies would have access to AR glasses data about them (Q5) said yes. Potential collectors and receivers about whom we prompted participants included the AR glasses company, employers, insurance companies, advertisers, doctors, researchers, and fitness apps. Participants raised concerns about unknown receivers, law enforcement (see details in Section 5.3), burglars, home attackers, kidnappers, hackers, someone you're trying to avoid, domestic violence abusers, and stalkers.

5.1.1 AR Glasses Company. A few participants expressed opinions regarding the AR glasses company. For example, P8 considered Apple to be "secure" and Amazon to be "a trusted brand," adding, "If it's a brand I'm unfamiliar with I wouldn't want them listening to my conversation" (Audio). P14 said they "wouldn't trust Facebook at all" because of their "spotty history" with privacy, but said they "might trust Google a little more" (Indoor Spaces). P19 expressed skepticism about AR companies deleting data:

> *Even if you delete your Facebook data, they'll just start a new tracker profile for you. . . . We don't have any real regulations, at least in the US, about whether that data is truly deleted. I would want to see some kind of regulation about that first, before I would even trust the feature. (P19, Q8: Deletion)*

P15 said their comfort transferring data across device brands would depend on if they agreed with each brand's storage policies (Q9).

5.1.2 Employers. Some participants were concerned about data being sent to employers. P7 was concerned about gestural data potentially being "mis-use[d]" by employers to flag people as suspicious (Movement). Similarly, P4 suggested consequences for perceived "aggressive" movements:

> *If I'm behaving a certain way at work, and this starts triggering something, . . . like, oh, she must be aggressive, the way she's waving her hands. Now we're flagging your HR file. (P4, Movement)*

P12 appeared to note uneven benefits:

> *An employer, looking at the reaction time of all their employees and saying this person's really slow, they're getting fired, right, it seems to benefit external third parties more than the [data subject] (P12, Reaction Times)*

P11 suggested that employers' access to social feedback and mood or emotion data could be "bad for me, employee, but good for that business, because you know, I'm not improving their business." P14 was concerned about "employers reaching too far into the personal lives of employees" and suggested that employees might be pressured into sharing information (Social Feedback).

5.1.3 Insurance Companies. Even without being prompted by a negative example (Reaction Times), some participants expressed concerns about medical or life insurance companies increasing rates or denying coverage based on AR glasses data.

> *If the device decides that I am having seizures . . . does that mean like okay now I have pre-existing conditions and I can't get insurance? (P4, Health Monitoring)*

P4 said they would not want AR glasses to be able to automatically "report" health conditions to doctors and insurance companies.

5.1.4 Health Monitoring Data Receivers. About half of participants said they would share health monitoring data with doctors or other healthcare providers, researchers, and fitness apps. Some participants said they would share information with doctors if they were experiencing a serious health issue. A few expected this data to be protected by U.S. HIPAA law, and others noted they would not want it to be shared with insurance companies or a nationwide hospital system. When asked about sharing with researchers, participants were concerned about consent, the purpose of the research, how the data would be used, funding resources, who the researchers were, and secure storage of the data. Participants' concerns about fitness apps included whether they trusted the app or platform and if they could control who uses the data.

5.1.5 Advertisers. Most participants (n=14) anticipated advertisers becoming involved in their data flows, and a few were concerned that advertising could be excessive or annoying.

> *I wouldn't want targeted advertising in a virtual space, because I don't see the point. Why would you interrupt my virtual experience with something from the real world? (P9, Virtual Spaces)*

P5 said they did not want advertisers "to know what excites [them]" and "get more effective," or gain a deeper understanding about them, because they already found ads to be "intrusive" (Brain Waves). P10 expressed cynicism about advertisers' motivations to learn what would make users "respond with a knee jerk reaction" and exploit it to "get people to impulse buy something or get them irrationally angry about issues" (Reaction Times). P2 recalled feeling conflicted about making purchases in their mobile AR game:

> *Lately . . . should I be buying random cosmetics in Ingress? Probably not, but I do it, and if they're offering more, then I might consider buying more stuff. (P2, Virtual Spaces)*

P2 suggested such pressure could lead to "addiction," comparing it to Amazon's purchase suggestions.

5.2 Data Subjects

When perceiving themselves as the data subject, some participants expressed concerns about disclosing personal information and hoped that AR glasses data would be anonymized or used in aggregate across groups of users, rather than associated with a personalized data profile based on inputs such as "eating habits, shopping habits, [or] health activity" (P4, Brain Waves). A few specified desiring or expecting data about themselves to be encrypted.

Almost all participants (n=18) expressed concern about bystanders' data being collected or used, mostly for the data types of face images, facial expressions, and bystanders' voiceprints, with eight participants suggesting that bystanders should be able to consent to data collection and a few suggesting that faces should be blurred, features should not work on other people, and facial recognition should be illegal. A few were concerned about the possibility of bystanders' data being collected by law enforcement, government, or security authorities (discussed in Section 5.3). P4 said they would be "worried" about "profiles that are being created about who I see and I interact with" (Face Images). Nevertheless, eight of 17 participants said they would use facial recognition on others, while only four of 16 said they would allow it to be used on them. Thus, more participants objected to being a subject of facial recognition than to being a collector. P14 thought data about other peoples' facial expressions could help them make a sale:

> *It might be useful for me to go back and see, if I was trying to make a sale … what people's reactions were to how I phrased various specific things. (P12, Facial Expressions)*

P14 and P16 suggested facial expression analysis could be used to detect lying in negotiations, depositions, and parenting.

5.3 Vulnerable Situations or Groups

We highlight below concerns about potential harms for people in vulnerable situations or groups. Some potential traits or situations mentioned by participants include: disability, non-standard accent or self-presentation, associating with or being near someone sought by law enforcement, dissenting or protesting, marginalized gender or sexual identity, and being a victim of stalking, abuse or theft.

Normative Biases. Some participants (n=12) suggested that discrimination could result from normative biases built into AR glasses features. For example, P7 was concerned about facial expression analysis on people who might not express themselves in normative ways, including autistic and other neurodiverse people:

> *Video analysis programs for use in hiring and video interviews, that is a real problem, that people who do not express their emotions typically can be flagged as untrustworthy or suspicious. I'm autistic. I don't necessarily express myself the same way that neurotypical people do. If my phone was paying attention to my facial expressions to try to judge my mood and respond in different ways, I feel like it just wouldn't work very well. (P7, Facial Expressions)*

P20 imagined a social feedback feature negatively assessing their non-standard American English accent from "rural Appalachia":

> *If the glasses are telling me that my accent is poor and that I need to retrain myself how to speak, that, I would have a bit of a bigger issue with. Having grown up in rural Appalachia, I can attest to the fact that an accent does not determine how intelligent or capable another person is. (P20, Social Feedback)*

Such concerns capture some potential AR glasses use cases that exclude minority or non-standard populations.

Criminal or Political Punishment. A few participants were concerned about authorities receiving AR glasses data and using it to target or harm people wanted for criminal or political activity. P4 was worried that face image data could cause them to set off a crime alert simply by observing a bystander who was sought by police, potentially "creating some sort of risk level" and profile for them (P4), as well as potentially involving them in the capture of an innocent person. P5 expressed concern that law enforcement's use of faulty facial recognition would result in "unfairly targeting the people that it's least able to recognize."

A few participants were concerned about AR glasses exposing users' or bystanders' political views, gender or sexual identity. P14 was concerned that attendees of meetings based on LGBT+ identity or political views could be identified via voice recordings:

> *I'm most nervous about, say, people who are LGBT plus and not out of the closet getting recorded at meetings. … Or political meetings, like everyone knows what happens in certain countries. (P14, Bystander Voiceprint)*

P20 suggested face image data of "political activists" could be collected at protests by "public security individuals" (P20, Face Images).

Personal Threat. Some participants (n=11) also expressed concerns about safety (their own or others'). Five participants mentioned the threat of stalking, and three were concerned about burglars. P7 expressed concern about inadvertently distributing information about a friend who had been stalked before:

> *I have friends who don't like having their pictures taken at all and don't want their pictures going on social media … İf I had glasses that did facial recognition, it would be kind of a betrayal of trust of those people. (P7, Face images)*

P14 evoked data risks faced by abuse victims in shelters:

> *[If someone] has one of these inside of a domestic violence shelter and isn't turning it off, that kind of thing, … the custodian of that data ends up being very important in that situation. (P14 Indoor Spaces)*

This suggests that AR glasses disclosing the location and identities of people in the shelter could endanger the user and others.

6 RESULTS: DESIRED PRIVACY PRINCIPLES (RQ3)

We present some privacy principles that participants expected or wished to apply to AR glasses data collection: user control, notice and consent, need-only use, and data protection. All 21 participants placed conditions on data collection or use, with conditions being noted across all categories a total of 125 times. The most common ones were notice (n=13), consent (n=19), and storage (n=16).

6.1 Individual User Control Over Data Flows

All participants expressed a wish to be able to customize or limit data collection, i.e., to enable or disable it, delete data, and control where and how data is stored. Most participants (n=16) wanted the ability to turn off certain features, and about half (n=10) wanted certain features to work only if initiated by the user.

> *If I couldn't stop it from recording everything, yeah, that's a hard no. (P10, Audio)*

P3 wished to control timing of data flows, to know "when" and "what data" was being sent to doctors and to not send "a constant stream of information to them" (Health Monitoring). P12 wanted granular control over "which data streams were being used" and was against brain wave data collection but would accept body temperature and heart rate data collection (Health Monitoring).

Ability to Delete. We asked nine participants whether the ability to delete their data made a difference (Q9), and eight said yes.

> *As the creator of that data, you should also have custody over that data and your right to have custody over that is also your right to delete it. (P20, Q9)*

Some participants were skeptical that they would even have this option, suspecting that their data would exist somewhere else anyway. Participants considered deletion useful for when they stopped using the device, wished to be forgotten (e.g., delete their social media account), and to delete data they did not find useful.

Storage. Most participants (n=16) also expressed concerns or reservations about storage and retention of the data. Six participants noted that they would rather have data be used temporarily and not saved or stored, with a few mentioning their home IoT devices having such options for ephemeral or temporary storage. When asked specifically about storage (Q6), 11 of 12 participants expressed a preference for data to be only stored locally on the device, not on a remote server ("in the cloud"), with a few participants being concerned about data breaches. P12 said they would have "low confidence that anything that happens on the cloud will stay truly private in perpetuity. P6 and P15 conditioned their comfort with cloud storage on encryption and hashing.

6.2 Notice and Consent

About half of participants (n=13) expressed a wish for notices. When asked about how they would want to be informed about who has access to their data (Q5), participants suggested being informed through an initial walk-through or notification, a settings menu, email, privacy documents, semi-regular reports, a website, or mobile and desktop apps. P15 wished for granular explanations about how health monitoring data would be used. Almost all participants (n=19) said they expected or desired a choice, i.e., to provide consent, opt in or out of data collection or certain features, or rescind or modify their consent, mentioning consent a total of 77 times for all data types and four data uses (all except Face Filter).

6.3 Need-only Use

A few participants acknowledged that some AR glasses data collection might be "necessary," and thus that users could sometimes lack meaningful choices, given no alternative except to not use the device. P19 suggested that users would not be able to opt out of eye tracking features, since disabling them might "make the device basically inoperable" (Eye Tracking). P4 objected to potential uses beyond the improving an application:

> *I would be okay with that, unless it's trying to create a behavior profile of me. . . . If it's a more generic sense, to understand how players or users of the system interact, to increase usability or productivity of the feature or device, that's fine. (P4, Virtual Spaces)*

Other participants also conditioned their comfort on whether data collection was necessary for the functioning of the feature or device.

6.4 Data Protection

Ten participants raised concerns about sensitive data content, across nine data types and two data uses, such as inferred income level, personal identity, sensitive conversations (with friends, family, romantic partners, coworkers, or in multi-player games), data profiles, certain images, and information collected while sleeping. Some participants suggested that legal protections should apply to certain data. Four participants felt biometric or health data should be protected by health privacy laws, e.g., HIPAA (U.S.):

> *There's already so many protections around medical data, I'm not too concerned about that. (P10, Health Monitoring)*

All 21 participants had concerns about recordings, for 12 data types and one data use. Three participants (P5, P7, P10) discussed potential unacceptability of recording, evoking U.S. state laws against recording without permission, which apply in what are known as All-Party or Two-Party consent states. A few participants expressed concerns about AR glasses violating confidentiality norms, such as intellectual property (IP) rules. P13 suggested a company's strategies or product information could be leaked.

> *Imagine another company trying to get . . . information by monitoring what employees are talking about. . . . That could be a disaster. It's literally a breach. (P13, Social Feedback)*

For this reason, P13 suggested that information collected in office settings be stored locally on the device "without being analyzed by a third party." P12 suggested AR glasses collecting indoor spaces data might violate a workplace policy by "giving away trade secrets." P4 raised concerns about ownership of voiceprints:

> *As long as I still own the rights. Like I don't want to go into a store and start hearing voiceover things in my voice. (P4, User Voiceprint)*

They opined that "a recording of Abraham Lincoln's voice . . . could be really cool" but wondered about the "rights" to Lincoln's voiceprint.

7 DISCUSSION

Our study reveals many diverse concerns and desired privacy standards for future AR glasses. Some of our findings are specific to AR glasses, due to the mobile form factor of a head-mounted display, the integration and combination of sensors (corresponding to our data types), and the potential for instantaneous analysis of these sensor inputs while moving in and engaging with the external environment. Here we bring together privacy concerns spanning different aspects of AR glasses data collection using a subset of Solove's taxonomy of privacy harms. We also discuss the context-relevant nature of participants' concerns, consider the privacy implications of potential mitigations for concerns about vulnerable situations or groups, and compare our findings to prior work. Finally, we make recommendations for privacy legislation and AR glasses design.

7.1 Privacy Harms

We apply Solove's privacy harms taxonomy [93] to the concerns raised by participants, noting which problems from the taxonomy's four groups the participants discussed. In comparison to features of widely available devices like mobile phones, several of these could be relatively unique to AR glasses, such as combined video feed, input from multiple sensors, and network connectivity, as well as features like reaction times, brain wave data, facial expression analysis, and overlain advertisements.

Information collection. First, participants raised concerns about potentially harmful information collection, specifically the problem of surveillance, such as recording private conversations or activities, tracking brain wave data and correlated visual material, and employers monitoring reaction times of their employees.

Information processing. Participants also expressed concerns about all of Solove's information processing problems: aggregation, identification, insecurity, secondary use, and exclusion. Given the multiple sensors of AR glasses and its potential network connectivity, participants suggested various pieces of data about them might be aggregated, such as external sensor data (e.g., video or audio) and biometric data, which could be used to make inferences about users. Identification, or "linking information to particular individuals," was also a concern, especially in virtual spaces or via facial recognition. Regarding storage, some participants suspected problems of insecurity, which Solove defines as "carelessness in protecting stored information from leaks and improper access," expressing a wish for data to be stored temporarily, be deletable, and also to be stored on-device only. Secondary use ("the use of information collected for one purpose for a different purpose without the data subject's consent") came up several times, as participants expressed concerns about health monitoring data being sent to insurance companies who might deny them insurance based on pre-existing conditions, brain wave data being used to recommend medical treatments or products, and recordings being used by third parties. Exclusion, or failure to inform the data subject about data collected or used about them and to involve them in its handling and use, was a problem raised about bystanders as well as about users whose data might be collected by unknown receivers and used for unknown purposes. Many participants wished to know who would have access to their data and how it would be used.

Information dissemination. Participants were concerned about problems related to information dissemination, including the problems of breach of confidentiality, disclosure, exposure, appropriation, and distortion. Breach of confidentiality ("breaking a promise to keep a person's information confidential") was raised as a potential problem in work settings, where AR glasses might cause proprietary information to be leaked. Disclosure ("revelation of truthful information about a person that impacts the way others judge her character") was a concern regarding marginalized identities, such as LGBTQ status, disclosure of negative feelings using facial expression analysis, as well as health conditions, such as worsening health. Some worried about potentially pervasive AR glasses data collection resulting in exposure ("revealing another's nudity, grief, or bodily functions") of activities they considered private, such as bathroom use or physical intimacy. Participants concerned about appropriation ("the use of the data subject's identity to serve the aims and interests of another") suggested that bystander data and voiceprints could be appropriated to serve the glasses user or corporate interests. The problem of distortion ("dissemination of false or misleading information about individuals") arose when discussing data that could be misinterpreted and used by employers, such as brain wave, movement, or facial expression data.

Invasion. Some participants expressed concern about privacy invasions such as intrusion (disturbance of tranquility), fearing that AR glasses would pester them with advertisements or personalized recommendations, including behavioral modification suggestions, or wishing to limit data collection in private spaces or contexts.

7.2 Context-Dependent Privacy Considerations

The range of privacy contexts and concerns provided by participants, even with a small group of people, suggests that it would be difficult to design satisfactory static and predetermined privacy options. While some participants invoked the private/public dichotomy, dividing privacy spheres into two contexts [75, 107], as a basis for constraining data flows, others provided contexts that do not fit into a binary private/public separation of places or activities, such as virtual spaces, the act of recording, or sensitive conversations. Given such contextual dependencies, we encourage researchers and AR professionals to apply the privacy framework of contextual integrity [75, 76] to study AR glasses privacy concerns in specific contexts, to better explore factors such as stakeholders and sociocultural norms, and to discover and articulate information norms, which Nissenbaum defines using the elements of data types, senders, receivers, subjects, and transmission principles—some of which coincide with topics of concern in our study.

While a norms-based approach to privacy can be useful for establishing baseline online privacy norms rooted in physical social life, Nissenbaum acknowledges that such a framework "appears to provide no buffer against insidious shifts in practice that ultimately gain acceptance as 'normal.'" In our study, participants sometimes expressed discomfort with entrenched data practices, such as advertisers receiving their data, employee monitoring, always-on functionality, and recording of bystanders. Yet, they varied in expressing resignation or a desire for alternatives. A way to avoid further entrenching unwarranted or "tyrannical" normative practices is by comparing these entrenched practices "against novel alternatives or competing practices on the basis of how effective each is in supporting, achieving, or promoting relevant contextual values" [75]. Thus, future work could explore establishing novel alternatives to entrenched norms that better embody relevant contextual values. Articulating what these contextual values are is also a space for future work, since values can fluctuate in online settings based on factors such as who has access to information, who the information is intended for, and technological privacy affordances [63].

7.3 Potential Exclusion or Discrimination

Some participants raised concerns about AR glasses data collection potentially resulting in exclusion, marginalization, or discrimination, e.g., features that apply normative biases to users with disabilities or nonstandard accents could alienate or marginalize them, especially in the contexts of hiring interviews or social feedback.

Future work should explore potential mitigations for such discrimination and their privacy implications. For example, if mitigations are developed to detect or to take as input factors such as disability or dialect, such that the product could adapt to these factors, what are the potential privacy protections that could be placed to prevent this data from being further distributed or used? Also, if AR glasses are able to detect medical conditions and social, linguistic, or demographic information about users, designers and researchers should consider potential harms of unintentional disclosure or false positives of detected features.

Our findings also suggest political and humanitarian implications for AR glasses data policies: dissenters, protesters, LGBT+ people, and innocent suspects were given as examples of people who might be at risk of persecution or punishment if AR glasses data were to be used against them in certain contexts. Additionally, a few participants evoked the norm of anonymity in virtual contexts that permits a certain freedom of behavior or interaction and suggested that mandating disclosure of or exposing identifying information could pose privacy and security risks to people in vulnerable situations or groups. Yet, designers must also contend with the potential for exclusionary norms or harassment in such spaces (see Section 2).

7.4 Comparing Findings to Prior Work

As in prior work on AR glasses privacy concerns, the purpose of data collection or use was a major concern for participants [51], as was recording, with some participants evoking laws against recordings [18, 51, 55]. Similar to findings in Koelle et al.'s work on social acceptability of data glasses, participants responded differently based on whether they considered themselves the user or the subject (in our case, of facial recognition) [51], as well as whether they made the choice to provide information or not [86]. Unlike most prior work, our study provides an analysis of the privacy concepts or problems evoked by participants. Our focus on data collection allowed participants to provide concerns about specific data types and articulate objections to particular data flows that were not specified in prior work that specified privacy concepts [78].

7.5 Recommendations

Design. Participants' privacy wishes and expectations vary significantly, even among 21 participants. Designing for millions of people will surely invite even more complex considerations. Additionally, some challenges (e.g., overlaid advertisements, expression analysis) are new enough that we believe substantial additional research is needed before we can develop designs to address them. Participants' varying levels of comfort based on diverse factors suggest that AR professionals should create flexible privacy choices to meet complex privacy considerations, such as customizable user controls over data flows and the ability to opt out of data collection. There is ample opportunity to provide AR glasses users with choices about data collection, use, and storage, for example, as proposed in prior work [19, 45]. We also recommend designing for adaptive privacy considerations, based on dynamic factors such as the varied privacy needs of people present in the same physical location or virtual context.

Most participants wished to receive detailed information about how their information is used, who receives it, and where it is stored. Many AR/VR glasses and applications already require personally identifiable data for functionality [49]. In such situations, users may not be granted means to control or regulate certain data flows, but notice and consent mechanisms should provide transparency regarding data collection, use, sharing, and storage. Harborth et al. found that contextualized justifications for mobile AR app permissions reduce privacy concerns and increase the willingness to grant permissions [33]. This suggests that contextualizing data collection and use by providing details about intended functionalities and data access could assuage user concerns about opaque or nefarious data flows. However, being transparent about excessive data collection or violations of privacy norms may not necessarily reduce privacy concerns, and managing the intensity and frequency of notifications is an ongoing issue in privacy notice and consent interfaces.

Legal Protections. We anticipate invasive products that test users' privacy boundaries. Most participants expected or imagined scenarios in which their data was collected or accessed by private actors such as the AR company, advertisers, and their employers. Some expressed discomfort regarding potentially opaque data use and data storage practices. A few participants expected health-related data and recordings to be protected under HIPAA (which only covers data used in a healthcare context) or All-Party recording laws (which vary by state and may not protect biometric information). Recent litigation under laws such as Illinois's Biometric Information Privacy Act has suggested that regulation can be effective in moving companies to develop options for transparency and consent [11, 83]. Without robust privacy laws, production of knowledge and recommendations about potential users' concerns and limits is not likely to result in better protection for consumers [20, 56, 79]. Our study confirms the multi-faceted nature of privacy, with participants expressing concerns that cannot be addressed by one-dimensional definitions of privacy. We therefore recommend that policy makers enact regulations for data collection, data protection, user control and disclosure, as well as laws that, like HIPAA, enforce privacy norms for data flows in settings where privacy is socially mandated.

8 CONCLUSION

Our exploratory study analyzed data from 21 interviews regarding data collection and use by hypothetical future AR glasses. We consider participants' privacy concerns and desired privacy principles, which are varied and context-dependent. We connect these results to privacy concepts and call for multifaceted solutions.

ACKNOWLEDGMENTS

We thank the anonymous reviewers for their comments. This research was funded in part by Meta.

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 (SOUPS 2018).* https://www.usenix.org/conference/soups2018/presentation/adams

[2] Sami Alkhatib, Ryan Kelly, Jenny Waycott, George Buchanan, Marthie Grobler, and Shuo Wang. 2021. "Who Wants to Know all this Stuff?!": Understanding

Older Adults' Privacy Concerns in Aged Care Monitoring Devices. *Interacting with Computers* 33, 5 (2021), 481–498. https://doi.org/10.1093/itnow/bwac034
[3] Anita L. Allen. 2011. *Unpopular Privacy: What Must We Hide?* Oxford University Press, New York.
[4] Apple. 2022. Legal - Apple Privacy Policy - Apple. https://www.apple.com/legal/privacy/en-ww/ Accessed June 9, 2023.
[5] Apple. 2023. Introducing Apple Vision Pro. https://www.apple.com/newsroom/2023/06/introducing-apple-vision-pro/
[6] Apple. 2023. Legal - Data & Privacy - Apple. https://www.apple.com/legal/privacy/data/ Accessed June 9, 2023.
[7] Noah Apthorpe, Sarah Varghese, and Nick Feamster. 2019. Evaluating the Contextual Integrity of Privacy Regulation: Parents' IoT Toy Privacy Norms Versus COPPA. In *28th USENIX Security Symposium (USENIX Security 19)*. https://www.usenix.org/conference/usenixsecurity19/presentation/apthorpe
[8] Arif Bacchus. 2019. Microsoft HoloLens 2 Hands-On Review. *Digital Trends* (Nov 2019). https://www.digitaltrends.com/computing/microsoft-hololens-2-ar-hands-on-features-price-photos-video-release-date/ Accessed November 30, 2022.
[9] Deepti Balaji Raykar and V Sridhar. 2022. Elicitation of Personal Data Categories for Implementing Data Protection: An Exploratory Study in an Educational Institution. In *15th Innovations in Software Engineering Conference* (Gandhinagar, India) *(ISEC 2022)*. Article 15. https://doi.org/10.1145/3511430.3511443
[10] Mary Elizabeth Ballard and Kelly Marie Welch. 2017. Virtual Warfare: Cyberbullying and Cyber-Victimization in MMOG Play. *Games and Culture* 12, 5 (2017). https://doi.org/10.1177/1555412015592473
[11] Kristin L. Bryan, Christina Lamoureux, and Dan Lonergan. 2022. 2021 Year in Review: Biometric and AI Litigation. *The National Law Review* (5 January 2022). https://www.natlawreview.com/article/2021-year-review-biometric-and-ai-litigation
[12] Kent Bye, Diane Hosfelt, Sam Chase, Matt Miesnieks, and Taylor Beck. 2019. The ethical and privacy implications of mixed reality. In *ACM SIGGRAPH 2019 Panels*. https://doi.org/10.1145/3306212.3328138
[13] Chola Chhetri and Vivian Motti. 2022. "I mute my echo when I talk politics": Connecting Smart Home Device Users' Concerns to Privacy Harms Taxonomy. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 66. SAGE Publications. https://doi.org/10.1177/1071181322661114
[14] HTC Corporation. 2022. Privacy Policy | Terms | HTC United States. https://www.htc.com/us/terms/privacy/ Accessed November 30, 2022.
[15] HTC Corporation. 2022. Vive Legal Documents | HTC United States. https://www.htc.com/us/terms/vive/ Accessed November 30, 2022.
[16] Amanda C Cote. 2017. "I Can Defend Myself": Women's Strategies for Coping With Harassment While Gaming Online. *Games and Culture* 12, 2 (2017). https://doi.org/10.1177/1555412015587603
[17] Jaybie A. De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. 2019. Security and Privacy Approaches in Mixed Reality: A Literature Survey. *ACM Comput. Surv.* 52, 6 (2019). https://doi.org/10.1145/3359626
[18] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. 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)*. https://doi.org/10.1145/2556288.2557352
[19] John J. Dudley, Jason T. Jacques, and Per Ola Kristensson. 2021. Crowdsourcing Design Guidance for Contextual Adaptation of Text Content in Augmented Reality. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3411764.3445493
[20] Ben Egliston and Marcus Carter. 2022. 'The metaverse and how we'll build it': The political economy of Meta's Reality Labs. *New Media & Society* (2022). https://doi.org/10.1177/14614448221119785
[21] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring how privacy and security factor into IoT device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3290605.3300764
[22] Rose Eveleth. 2018. Google Glass Wasn't a Failure. It Raised Crucial Concerns. *Wired* (2018). https://www.wired.com/story/google-glass-reasonable-expectation-of-privacy/
[23] Cori Faklaris, Asa Blevins, Matthew O'Haver, Neha Singhal, and Francesco Cafaro. 2017. An Exploration of User and Bystander Attitudes About Mobile Live-Streaming Video. (2017). https://doi.org/10.13140/RG.2.2.14052.22406
[24] Ben Falchuk, Shoshana Loeb, and Ralph Neff. 2018. The Social Metaverse: Battle for Privacy. *IEEE Technology and Society Magazine* 37, 2 (2018). https://doi.org/10.1109/MTS.2018.2826060
[25] Guo Freeman, Divine Maloney, Dane Acena, and Catherine Barwulor. 2022. (Re)discovering the Physical Body Online: Strategies and Challenges to Approach Non-Cisgender Identity in Social Virtual Reality. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3491102.3502082
[26] Yang Gao, Yincheng Jin, Jagmohan Chauhan, Seokmin Choi, Jiyang Li, and Zhanpeng Jin. 2021. Voice In Ear: Spoofing-Resistant and Passphrase-Independent Body Sound Authentication. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5, 1 (2021). https://doi.org/10.1145/3448113
[27] Kathrin Gerling and Katta Spiel. 2021. A Critical Examination of Virtual Reality Technology in the Context of the Minority Body. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3411764.3445196
[28] Google. 2014. Glass Terms of Use. https://www.google.com/glass/termsofuse/ Accessed November 30, 2022.
[29] Google. 2015. Wearable emotion detection and feedback system - Google Patents. https://patents.google.com/patent/US9508008B2/en
[30] Google. 2022. Google Privacy Policy. https://policies.google.com/privacy Accessed November 30, 2022.
[31] Marco Guermandi, Simone Benatti, Victor Javier Kartsch Morinigo, and Luca Bertini. 2018. A Wearable Device for Minimally-Invasive Behind-the-Ear EEG and Evoked Potentials. In *2018 IEEE Biomedical Circuits and Systems Conference (BioCAS)*. https://doi.org/10.1109/BIOCAS.2018.8584814
[32] Jisoo Ha, Seonghun Park, and Chang-Hwan Im. 2022. Novel Hybrid Brain-Computer Interface for Virtual Reality Applications Using Steady-State Visual-Evoked Potential-Based Brain–Computer Interface and Electrooculogram-Based Eye Tracking for Increased Information Transfer Rate. *Frontiers in Neuroinformatics* 16 (2022). https://doi.org/10.3389/fninf.2022.758537
[33] David Harborth and Alisa Frik. 2021. Evaluating and Redefining Smartphone Permissions with Contextualized Justifications for Mobile Augmented Reality Apps. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. https://www.usenix.org/conference/soups2021/presentation/harborth
[34] David Harborth and Sebastian Pape. 2021. Investigating privacy concerns related to mobile augmented reality Apps–A vignette based online experiment. *Computers in Human Behavior* 122 (2021). https://doi.org/10.1016/j.chb.2021.106833
[35] Scharon Harding. 2022. Lenovo announces consumer AR glasses that can tether to iPhones. *Ars Technica* (Sep 2022). https://arstechnica.com/gadgets/2022/09/lenovos-first-consumer-ar-glasses-to-debut-this-year-with-micro-oled-displays/ Accessed November 30, 2022.
[36] Chris Harrison and Haakon Faste. 2014. Implications of Location and Touch for On-Body Projected Interfaces. In *Proceedings of the 2014 Conference on Designing Interactive Systems*. https://doi.org/10.1145/2598510.2598587
[37] Woodrow Hartzog. 2021. What is Privacy? That's the Wrong Question. *The University of Chicago Law Review* 88 (2021), 1677.
[38] Jason Hong. 2013. Privacy and Google Glass. https://cacm.acm.org/blogs/blog-cacm/167230-privacy-and-google-glass/fulltext Accessed November 30, 2022.
[39] Roberto Hoyle, Robert Templeman, Denise Anthony, David Crandall, and Apu Kapadia. 2015. Sensitive Lifelogs: A Privacy Analysis of Photos from Wearable Cameras. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/2702123.2702183
[40] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy behaviors of lifeloggers using wearable cameras. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. https://doi.org/10.1145/2632048.2632079
[41] Magic Leap Inc. 2020. Privacy Policy. https://resources.magicleap.com/en-us/privacy/privacy-policy Accessed November 30, 2022.
[42] Magic Leap Inc. 2022. Magic Leap 2 full technology specifications. https://www.magicleap.com/magic-leap-2 Accessed November 30, 2022.
[43] Snap Inc. 2022. Privacy Policy. https://snap.com/en-US/privacy/privacy-policy Accessed November 30, 2022.
[44] Snap Inc. 2022. Spectacles 3: Tech Specs. https://www.spectacles.com/shop/spectacles-3 Accessed November 30, 2022.
[45] Suman Jana, David Molnar, Alexander Moshchuk, Alan Dunn, Benjamin Livshits, Helen J. Wang, and Eyal Ofek. 2013. Enabling Fine-Grained Permissions for Augmented Reality Applications with Recognizers. https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/jana
[46] Patrick Gage Kelley, Michael Benisch, Lorrie Faith Cranor, and Norman Sadeh. 2011. When Are Users Comfortable Sharing Locations with Advertisers?. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/1978942.1979299
[47] Suleman Khan, M. Hammad Javed, Ehtasham Ahmed, Syed A A Shah, and Syed Umaid Ali. 2019. Facial Recognition using Convolutional Neural Networks and Implementation on Smart Glasses. In *2019 International Conference on Information Science and Communication Technology (ICISCT)*. https://doi.org/10.1109/CISCT.2019.8777442
[48] Dokyun Kim, Wooseok Byun, Yunseo Ku, and Ji-Hoon Kim. 2019. High-Speed Visual Target Identification for Low-Cost Wearable Brain-Computer Interfaces. *IEEE Access* 7 (2019). https://doi.org/10.1109/ACCESS.2019.2912997
[49] Yeji Kim. 2022. Virtual Reality Data and Its Privacy Regulatory Challenges: A Call to Move Beyond Text-Based Informed Consent. *California Law Review* 110, 1 (2022).
[50] Marion Koelle, Abdallah El Ali, Vanessa Cobus, Wilko Heuten, and Susanne CJ Boll. 2017. All about Acceptability? Identifying Factors for the Adoption of Data Glasses. In *Proceedings of the 2017 CHI Conference on Human Factors in*

Computing Systems. https://doi.org/10.1145/3025453.3025749
[51] Marion Koelle, Matthias Kranz, and Andreas Möller. 2015. Don't look at me that way! Understanding User Attitudes Towards Data Glasses Usage. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*. https://doi.org/10.1145/2785830.2785842
[52] Jacob Leon Kröger, Otto Hans-Martin Lutz, and Florian Müller. 2019. What does your gaze reveal about you? On the privacy implications of eye tracking. In *IFIP International Summer School on Privacy and Identity Management*. https://doi.org/10.1007/978-3-030-42504-3_15
[53] Jangho Kwon, Jihyeon Ha, Da-Hye Kim, Jun Won Choi, and Laehyun Kim. 2021. Emotion Recognition Using a Glasses-Type Wearable Device via Multi-Channel Facial Responses. *IEEE Access* 9 (2021). https://doi.org/10.1109/ACCESS.2021.3121543
[54] Lutz Lammerding, Tim Hilken, Dominik Mahr, and Jonas Heller. 2021. Too real for comfort: Measuring consumers' augmented reality information privacy concerns. In *Augmented Reality and Virtual Reality: New Trends in Immersive Technology*. Springer, 95–108.
[55] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2018. Towards Security and Privacy for Multi-user Augmented Reality: Foundations with End Users. In *2018 IEEE Symposium on Security and Privacy (SP)*. https://doi.org/10.1109/SP.2018.00051
[56] Daniel Leufer. 2021. Privacy review of Facebook's Ray-Ban Stories smart glasses. *Access Now* (Sep 2021). https://www.accessnow.org/facebook-ray-ban-stories-smart-glasses-privacy-review/ Accessed November 30, 2022.
[57] Huining Li, Chenhan Xu, Aditya Singh Rathore, Zhengxiong Li, Hanbin Zhang, Chen Song, Kun Wang, Lu Su, Feng Lin, Kui Ren, and Wenyao Xu. 2020. VocalPrint: Exploring a Resilient and Secure Voice Authentication via MmWave Biometric Interrogation. In *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*. https://doi.org/10.1145/3384419.3430779
[58] Kai Li, Zhangxi Lin, and Xiaowen Wang. 2015. An empirical analysis of users' privacy disclosure behaviors on social network sites. *Information & management* 52, 7 (2015), 882–891. https://doi.org/10.1016/j.im.2015.07.006
[59] Daniel J. Liebling and Sören Preibusch. 2014. Privacy Considerations for a Pervasive Eye Tracking World. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*. https://doi.org/10.1145/2638728.2641688
[60] Xiao Ma, Jeff Hancock, and Mor Naaman. 2016. Anonymity, Intimacy and Self-Disclosure in Social Media. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/2858036.2858414
[61] Angus Main and Dylan Yamada-Rice. 2022. Evading Big Brother: Using visual methods to understand children's perception of sensors and interest in subverting digital surveillance. *Visual Communication* 21, 3 (2022). https://doi.org/10.1177/14703572221093559
[62] Divine Maloney, Samaneh Zamanifard, and Guo Freeman. 2020. Anonymity vs. Familiarity: Self-Disclosure and Privacy in Social Virtual Reality. In *26th ACM Symposium on Virtual Reality Software and Technology*. https://doi.org/10.1145/3385956.3418967
[63] Alice E Marwick and Danah Boyd. 2014. Networked privacy: How teenagers negotiate context in social media. *New media & society* 16, 7 (2014), 1051–1067. https://doi.org/10.1177/1461444814543999
[64] Katsutoshi Masai, Yuta Sugiura, Masa Ogata, Kai Kunze, Masahiko Inami, and Maki Sugimoto. 2016. Facial Expression Recognition in Daily Life by Embedded Photo Reflective Sensors on Smart Eyewear. In *Proceedings of the 21st International Conference on Intelligent User Interfaces*. https://doi.org/10.1145/2856767.2856770
[65] Nora McDonald and Andrea Forte. 2020. The Politics of Privacy Theories: Moving from Norms to Vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3313831.3376167
[66] Lavinia McLean and Mark D Griffiths. 2019. Female Gamers' Experience of Online Harassment and Social Support in Online Gaming: A Qualitative Study. *International Journal of Mental Health and Addiction* 17, 4 (2019), 970–994. https://doi.org/10.1007/s11469-018-9962-0
[67] Meta. 2022. Hand tracking privacy notice. https://store.facebook.com/en-gb/help/quest/articles/accounts/privacy-information-and-settings/hand-tracking-privacy-notice/ Accessed November 30, 2022.
[68] Meta. 2022. Monitoring and recording safety Horizon | Meta Quest. https://store.facebook.com/de/en/legal/quest/monitoring-recording-safety-horizon/ Accessed November 30, 2022.
[69] Meta. 2022. Oculus Privacy Policy | Meta Quest. https://store.facebook.com/de/en/legal/quest/updated-privacy-policy-for-oculus-account-users/ Accessed November 30, 2022.
[70] Meta. 2022. Privacy information and settings. https://store.facebook.com/en-gb/help/quest/articles/accounts/privacy-information-and-settings/ Accessed November 30, 2022.
[71] Microsoft. 2022. HoloLens 2 hardware. https://docs.microsoft.com/en-us/hololens/hololens2-hardware Accessed November 30, 2022.
[72] Microsoft. 2022. Improve visual quality and comfort. https://learn.microsoft.com/en-us/hololens/hololens-calibration Accessed November 30, 2022.
[73] Anish Nag, Nick Haber, Catalin Voss, Serena Tamura, Jena Daniels, Jeffrey Ma, Bryan Chiang, Shasta Ramachandran, Jessey Schwartz, Terry Winograd, Carl Feinstein, and Dennis P. Wall. 2020. Toward Continuous Social Phenotyping: Analyzing Gaze Patterns in an Emotion Recognition Task for Children With Autism Through Wearable Smart Glasses. *Journal of Medical Internet Research* 22, 4 (2020). https://doi.org/10.2196/13810
[74] Helen Nissenbaum. 1997. Toward an approach to privacy in public: Challenges of information technology. *Ethics & Behavior* 7, 3 (1997), 207–219. https://doi.org/10.1207/s15327019eb0703_3
[75] Helen Nissenbaum. 2010. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books, Stanford, California.
[76] Helen Nissenbaum. 2011. A Contextual Approach to Privacy Online. *Daedalus* 140, 4 (2011). https://doi.org/10.1162/DAED_a_00113
[77] Fayika Farhat Nova, Michael Ann DeVito, Pratyasha Saha, Kazi Shohanur Rashid, Shashwata Roy Turzo, Sadia Afrin, and Shion Guha. 2021. "Facebook Promotes More Harassment": Social Media Ecosystem, Skill and Marginalized Hijra Identity in Bangladesh. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (Apr 2021). https://doi.org/10.1145/3449231
[78] 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. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 6, 4 (Jan 2023). https://doi.org/10.1145/3569501
[79] Thao Phan, Jake Goldenfein, Monique Mann, and Declan Kuch. 2022. Economies of Virtue: The Circulation of 'Ethics' in Big Tech. *Science as Culture* 31, 1 (2022). https://doi.org/10.1080/09505431.2021.1990875
[80] Blaine A. Price, Avelie Stuart, Gul Calikli, Ciaran Mccormick, Vikram Mehta, Luke Hutton, Arosha K. Bandara, Mark Levine, and Bashar Nuseibeh. 2017. Logging you, Logging me: A Replicable Study of Privacy and Sharing Behaviour in Groups of Visual Lifeloggers. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, 2 (2017). https://doi.org/10.1145/3090087
[81] Jason Procyk, Carman Neustaedter, Carolyn Pang, Anthony Tang, and Tejinder K. Judge. 2014. Exploring Video Streaming in Public Settings: Shared Geocaching over Distance Using Mobile Video Chat. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/2556288.2557198
[82] Cassidy Pyle, Lee Roosevelt, Ashley Lacombe-Duncan, and Nazanin Andalibi. 2021. LGBTQ Persons' Pregnancy Loss Disclosures to Known Ties on Social Media: Disclosure Decisions and Ideal Disclosure Environments. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3411764.3445331
[83] Katyanna Quach. 2021. McDonald's AI drive-thru bot accused of breaking biometrics privacy law. *The Register* (10 June 2021). https://www.theregister.com/2021/06/10/mcdonalds_ai_lawsuit/ Accessed June 15, 2023.
[84] Philipp A. Rauschnabel, Alexander Rossmann, and M. Claudia tom Dieck. 2017. An adoption framework for mobile augmented reality games: The case of Pokémon Go. *Computers in Human Behavior* 76 (2017). https://doi.org/10.1016/j.chb.2017.07.030
[85] Patrice Renaud, Joanne L Rouleau, Luc Granger, Ian Barsetti, and Stéphane Bouchard. 2002. Measuring sexual preferences in virtual reality: A pilot study. *CyberPsychology & Behavior* 5, 1 (2002), 1–9. https://doi.org/10.1089/109493102753685836
[86] Jan Ole Rixen, Mark Colley, Ali Askari, Jan Gugenheimer, and Enrico Rukzio. 2022. Consent in the Age of AR: Investigating The Comfort With Displaying Personal Information in Augmented Reality. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3491102.3502140
[87] Adi Robertson. 2021. Nreal Light review: Hardware is only half the battle. *The Verge* (Nov 2021). https://www.theverge.com/22791981/nreal-light-augmented-mixed-reality-glasses-review Accessed November 30, 2022.
[88] Franziska Roesner, Tadayoshi Kohno, and David Molnar. 2014. Security and privacy for augmented reality systems. *Commun. ACM* 57, 4 (2014). https://doi.org/10.1145/2580723.2580730
[89] Eric E Sabelman and Roger Lam. 2015. The real-life dangers of augmented reality. *IEEE Spectrum* 52, 7 (2015), 48–53. https://doi.org/10.1109/MSPEC.2015.7131695
[90] D Samuel. 1890. Warren & Louis D. Brandeis, The Right to Privacy. *Harvard Law Review* 4, 5 (1890), 193.
[91] Jocelyn Scheirer, Raul Fernandez, and Rosalind W. Picard. 1999. Expression glasses: a wearable device for facial expression recognition. In *CHI '99 Extended Abstracts on Human Factors in Computing Systems*. https://doi.org/10.1145/632716.632878
[92] Cong Shi, Xiangyu Xu, Tianfang Zhang, Payton Walker, Yi Wu, Jian Liu, Nitesh Saxena, Yingying Chen, and Jiadi Yu. 2021. Face-Mic: Inferring Live Speech and Speaker Identity via Subtle Facial Dynamics Captured by AR/VR Motion

Sensors. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*. https://doi.org/10.1145/3447993.3483272
[93] Daniel J Solove. 2006. A taxonomy of privacy. *University of Pennsylvania law review* (2006), 477–564.
[94] Daniel J. Solove. 2012. Introduction: Privacy Self-management and the Consent Dilemma. *Harvard Law Review* 126 (2012), 1880.
[95] Scott Stein. 2020. Varjo's lidar-enabled XR-3 VR headset shows where VR and AR are bound to blend. *CNET* (1 December 2020). https://www.cnet.com/tech/computing/varjos-lidar-enabled-xr-3-vr-headset-shows-where-vr-and-ar-are-bound-to-blend/ Accessed November 30, 2022.
[96] Scott Stein. 2021. Mind control comes to VR, letting me explode alien heads with a thought. *CNET* (Jan 2021). https://www.cnet.com/tech/computing/controlling-vr-with-my-mind-nextminds-dev-kit-shows-me-a-strange-new-world/ Accessed November 30, 2022.
[97] Leah Stodart. 2022. The best fitness trackers for keeping up with your goals. *Mashable* (Aug 2022). https://mashable.com/roundup/wearable-fitness-trackers-guide Accessed November 30, 2022.
[98] Philipp Sykownik, Divine Maloney, Guo Freeman, and Maic Masuch. 2022. Something Personal from the Metaverse: Goals, Topics, and Contextual Factors of Self-Disclosure in Commercial Social VR. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3491102.3502008
[99] Nishtha H. Tandel, Harshadkumar B. Prajapati, and Vipul K. Dabhi. 2020. Voice Recognition and Voice Comparison using Machine Learning Techniques: A Survey. In *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*. https://doi.org/10.1109/ICACCS48705.2020.9074184
[100] Wai Yen Tang and Jesse Fox. 2016. Men's harassment behavior in online video games: Personality traits and game factors. *Aggressive Behavior* 42, 6 (2016). https://doi.org/10.1002/ab.21646
[101] Matilde Tassinari, Matthias Burkard Aulbach, and Inga Jasinskaja-Lahti. 2022. The use of virtual reality in studying prejudice and its reduction: A systematic review. *PLOS ONE* 17, 7 (2022). https://doi.org/10.1371/journal.pone.0270748
[102] Hibby Thach, Samuel Mayworm, Daniel Delmonaco, and Oliver Haimson. 2022. (In)visible moderation: A digital ethnography of marginalized users and content moderation on Twitch and Reddit. *New Media & Society* (Jul 2022). https://doi.org/10.1177/14614448221109804
[103] Varjo. 2022. Eye tracking. https://varjo.com/use-center/get-to-know-your-headset/eye-tracking/ Accessed November 30, 2022.
[104] Varjo. 2022. Privacy Policy. https://varjo.com/privacy-policy/ Accessed November 30, 2022.
[105] Varjo. 2022. Terms of Service for Varjo XR-3 and VR-3. https://varjo.com/terms-of-service-for-varjo-xr-3-and-vr-3/ Accessed November 30, 2022.
[106] Varjo. 2022. Varjo and OpenBCI Partner to Bring Neurotechnology to Spatial Computing. https://varjo.com/company-news/openbci-and-varjo-partner-to-bring-neurotechnology-to-spatial-computing/ Accessed November 30, 2022.
[107] Michael Walzer. 1983. *Spheres of justice: A defense of pluralism and equality*. Basic Books.
[108] Frederike Wenzlaff, Peer Briken, and Arne Dekker. 2016. Video-based eye tracking in sex research: A systematic literature review. *The Journal of Sex Research* 53, 8 (2016). https://doi.org/10.1080/00224499.2015.1107524
[109] Te-Ping Chen Wu, Illustrations by Kevin Hand, and Development by Yan. 2021. Tech That Aims to Improve Meetings. *Wall Street Journal* (Jan 2021). https://www.wsj.com/articles/tech-that-aims-to-improve-meetings-11610640133 Accessed November 30, 2022.
[110] Jia Zhang, Yinian Zhou, Rui Xi, Shuai Li, Junchen Guo, and Yuan He. 2022. AmbiEar: MmWave Based Voice Recognition in NLoS Scenarios. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 6, 3. https://doi.org/10.1145/3550320
[111] Kexin Zhang, Elmira Deldari, Zhicong Lu, Yaxing Yao, and Yuhang Zhao. 2022. "It's Just Part of Me:" Understanding Avatar Diversity and Self-Presentation of People with Disabilities in Social Virtual Reality. In *Proceedings of the 24th International ACM SIGACCESS Conference on Computers and Accessibility*. https://doi.org/10.1145/3517428.3544829
[112] Shikun Zhang, Yan Shvartzshnaider, Yuanyuan Feng, Helen Nissenbaum, and Norman Sadeh. 2022. Stop the Spread: A Contextual Integrity Perspective on the Appropriateness of COVID-19 Vaccination Certificates. In *2022 ACM Conference on Fairness, Accountability, and Transparency*. https://doi.org/10.1145/3531146.3533222

A APPENDIX - RECRUITMENT TEXT

Below are the texts we used to recruit potential participants: the initial recruitment text and the follow-up email to people who filled out the screening survey.

A.1 Recruitment Text Posted to Reddit and Email Listserv

Recruiting for Carnegie-Mellon University Study on AR Technologies: 90-minute remote interview, $30 compensation

We are recruiting people with experience with augmented reality (AR) technologies for a research study. Each participant in the study will complete a remote interview over Zoom in which we will ask questions about your experiences with and thoughts about AR technologies. The study session will last approximately 90 minutes, and you will receive a $30 Amazon gift code as compensation after completing the interview. You may be eligible for this study if you meet the following criteria:

- You speak and understand English
- You are located in the U.S.
- You are at least 18 years old
- You can install and run Zoom for the interview
- You have used at least one augmented reality app or device recently. This could include any of the following, as well as other similar technologies: smartphone apps like Snapchat, Pokémon Go, Ingress, or Harry Potter: Wizards Unite or headsets or glasses such as Microsoft Hololens, Snapchat Spectacles, Google Glass, or Magic Leap 1

If you wish to participate, please complete our preliminary screening survey at [survey url]. If you are selected, one of our researchers will reach out to you for next steps. Thank you!

A.2 Consent form email distribution text (appended to Qualtrics distribution message)

Thank you for filling out the screening survey for our study on augmented reality (AR) glasses. Our study will be a 60-minute interview, conducted over a Zoom video conference. We will ask questions about your experiences with augmented reality technology, such as smartphone games or augmented reality headsets. After the study, you will be compensated with a $20 Amazon gift code. If you are still interested in participating, please fill out the consent form and let us know when you are available by selecting an available time through the Calendly link at the end of the consent form survey.

B APPENDIX - INTERVIEW SCRIPT

Below are the questions from our semi-structured interviews.

B.1 Questions about current AR use

B.1.1 Recent interaction details.

- Have you ever worked in a job that required you to use AR?
- Have you taken a course that focused significantly on AR?
- In the last year, have you worked on any AR projects, for example for work, school, or as a hobby?
- What AR technologies have you used within the past year?
- Do you use an AR headset? Regularly?
  - What do you use your device for?
  - Where do you use it?
- Which AR app or device of those do you use most frequently?

B.1.2 Current App/Device - Data Collection.

- What data do you think [app/device] is collecting about you?
  - What do you think this data is being used for?
  - How do you feel about this data collection?

B.2 General Attitudes and Expectations

- What would you like to do with AR glasses?
- What do you not want these AR glasses to be able to do?
- What things/data would you want AR glasses to collect/track?
- Is there any specific type of data you would not want AR glasses to collect or track?

B.3 Data Types - Harms & Benefits of Data Use

We have a list of 15 types of data that your AR glasses could collect about you or your surroundings. I will first ask you how you would feel about AR glasses collecting each type of data. For some we may ask you to consider potential benefits or potential harms of AR glasses collecting and using this data about you.

(1) Audio (Clarification: could be recordings, or could be always-on functionality, which would not store data long-term)
Benefit example: Send voice commands to glasses, for example, to schedule an appointment while doing activities where it is inconvenient to use hands, like driving, cooking, or running.
Harm example: Covertly record private conversations.

(2) Video or Image data (Clarification: could be recordings, or could be always-on functionality, which would not store data long-term) *Benefit example*: AR glasses could scan your fridge and cupboard contents to make a list of items you need, to help you figure out what you need to get at the store. *Harm example*: Live streaming a social event without peoples' consent could reveal someone's personal information, like their family's images, to an audience they don't know and wouldn't share with.

(3) Location data *Benefit example*: Navigational features like map directions. *Harm example*: Location data may reveal personal habits or relationships. Also, data mapped onto a virtual world could disclose personal information.

(4) Maps of indoor spaces (Clarification: interior spaces of buildings) *Benefit example*: Furniture shoppers could see where a new piece of furniture would fit in their living room. *Harm example*: Prices and targeted advertising for online products could change because third party apps make assumptions based on home interiors, for example, based on objects you have.

(5) Virtual spaces or virtuals locations that you have visited (spaces do not actually exist, e.g., VR Chat chatrooms, game worlds) *Benefit example*: A glasses user could keep a quick-access list of all the virtual spaces they like to visit so that they don't have to search every time. *Harm example*: Advertisements based on most-visited virtual spaces could pressure someone into making in-world add-on purchases that they later regret.

(6) Your heart rate *Benefit example*: The glasses could alert users to heart conditions like heart arrhythmia, which could cause them to take steps to prevent potential health problems. *Harm example*: A record of heart rate activity could disclose patterns like sleep, exercise, and moments of anxiety or excitement. If someone shares this, it will reveal a lot of personal information.

(7) Your body temperature *Benefit example*: Check for a fever to determine whether or not to leave home. *Harm example*: False positives, for example caused by using the device after being in contact with something hot, could result in automatic exclusion from events that screen for high temperatures.

(8) Your brain waves (neural oscillations) *Benefit example*: Help detect any potentially harmful brain activities, such as strokes, seizures, sleep disorders, or other brain issues. *Harm example*: Brain wave data aligned with visual data could be analyzed and potentially disclose personal info such as whether someone has seizures or make conclusions, such as recognizing someone.

(9) Data about how you move, for example, gait (how you walk), posture, physical gestures, or body language *Benefit example*: The glasses could regularly remind users to realign their posture to help prevent long-term back issues and allow for gestural controls that work for users. *Harm example*: The glasses could read body language reactions to certain statements, people, or situations and make predictions about how the person will react to similar information in the future, making them more susceptible to targeted advertising based on their body language.

(10) Eye tracking (your eyes) *Benefit example*: As someone reviews slides, art, or an event that they need to understand, they can see what they previously focused on (where their eyes looked) and discover things that they missed or barely acknowledged. *Harm example*: Companies might figure out what usually draws a person's attention and make conclusions about them.

(11) Face images (remembering other people's faces) *Benefit example*: A glasses user can be reminded of someone's name as they walk towards them, just in time for them to offer a personal greeting. *Harm example*: Strangers will learn personal details about each other, which many people might consider invasive.

(12) Facial expressions (yours and other people's) *Benefit example*: For someone using avatars or face filters, the glasses could sync their facial expressions with their avatar's face or a face filter. *Harm example*: Companies might analyze your facial expressions to see when you are most susceptible to marketing messages.

(13) Your voiceprint, including tone and pitch of your voice *Benefit example*: The device owner's voice could be used to unlock device features, in other words, no one but that person could unlock the features. *Harm example*: The device or apps could share your voiceprint with third parties.

(14) Other people's voiceprints, including tone and pitch *Benefit example*: Friends-only features could be unlocked in virtual spaces, where the space owner allows only certain people to access those features using their voices. *Harm example*: Deep fake applications that capture and imitate voices could enable

people to fool others by sending audio messages pretending to be someone else.

(15) Your reaction times, e.g. the amount of time you take to respond to a prompt *Benefit example*: Reaction times could be used to measure performance and help you improve performance, determine implicit attitudes, revealing unconscious biases, and action can be taken to avoid negative consequences. For example, a company realizes their hiring manager appears to automatically reject certain types of job applicants, so they change their practices to fairly evaluate such candidates. *Harm example*: Reaction times used to measure performance could result in burdensome consequences. For example, a student might be labeled a poor performer for slow reaction times, or a driver might be charged more for insurance for being slow on breaking. Alternatively could prove you were quick on breaks.

B.4 Data Use

For the following questions, provide a counterexample if their reaction is positive or negative and see how they respond. Now we will talk about a few use cases that we came up with and ask for your opinion. There may be some overlap with what we just talked about, so please bear with us if there is some repetition.

(1) How would you feel about notifications or reminders triggered by data being collected by the AR glasses, such as something you're looking at? *Benefit example*: a reminder that your pick-up order is ready as you walk by a store. *Harm example*: reminders could distract you when you are trying to focus or relax.
   (a) Do you feel this way about other reminders or notifications, like the ones on your phone or computer?
   (b) Would you like for your AR glasses to be able to predict what types of reminders would be helpful for you?

(2) How would you feel about using AR glasses to monitor health, based on sensor data, like body and movement data? (*Benefit example*: Track vitals and detect dangerous irregularities before a potentially dangerous condition develops. Could get discounts based on positive data. *Harm example*: An app may share health information with insurance companies or the government, which may change rates or services based on data.)
   (a) Would you be willing to share AR glasses data about your health with doctors or other healthcare providers?
   (b) With researchers?
   (c) With a fitness tracker app?

(3) How would you feel about using AR glasses for social or conversation feedback, such as how you speak, who you lean towards, or whether you interrupted someone? (*Benefit example*: Someone gets useful feedback on the tone of their voice as they practice a speech. *Harm example*: An employee gets negative evaluation from an AI tool that rates their conversation skills.)

(4) How would you feel about setting a face filter in AR so that other glasses users could only see you with the face filter? (*Benefit example*: Make friends laugh with amusing filters. *Harm example*: Some people may get body dysmorphia and stop presenting their real faces, wishing to look like filters or avatars)

(5) What do you think about AR glasses data being used to inform you about your mood or emotions? (*Benefit example*: During a conversation, someone gets feedback on their screen that they sound irritated, so they change their tone to sound calm, which leads to a more pleasant conversation. *Harm example*: Someone struggling to express themselves clearly becomes dependent on apps that inform them of their tone while they speak.)

(6) Would you use the facial recognition feature?
   - Would you allow other people with AR glasses to use facial recognition on you?

(7) Based on the types of data we talked about, can you think of any other features you might expect AR glasses to have?
   - Would you want this/these?

B.5 General Questions - Data Collection

(1) Does the location or where AR glasses collect data make a difference to you, e.g., whether you're out in public or at home?

(2) Does the time of day, or when they could collect data make a difference to you?

(3) Would data collection in certain social contexts make a difference to you, e.g. weddings, medical offices or places of worship?

(4) Would you like to have control over who else the glasses could collect data about?

(5) Would you like to know who or what companies would have access to data about you?
   - How would you like to be informed about that?

(6) Would it make a difference to you if the data was stored locally, only on the device, on your personal cloud, on the company cloud, or somewhere else?

(7) Does the length of time it is being stored make a difference to you?
   - *[If yes]* What length of time would make you uncomfortable for it to be stored?

(8) Would you like to be able to delete your AR glasses data?
   - How important is this to you?

(9) Would you like to be able to transfer your AR glasses data, e.g., from one brand of device to a different brand of device?
   - How do you imagine using this ability to transfer data?

(10) When would you like to be informed about data collection? Before? While using? After? Some mix?

(11) What would you like to know when you're being informed about data collection?

C APPENDIX - CODEBOOK

Below we include a copy of our code book containing the attitude codes and the emergent codes we used and developed throughout our qualitative coding process.

Attitude	Definition	Statements/Keywords
Comfortable/support	Participant either said they would be comfortable, expressed enthusiasm with no hesitation, or expressed explicit support. If hesitation was expressed, ratio was 1/3 of enthusiasm or less, or expressed as an afterthought. Qualified with Would Use. If coded Would Not Use, still expressed explicit support; otherwise label as Uncomfortable. If they sympathize with negative, still express comfort or support personally. Condition for non-use is very minor. Compares to something they're already comfortable with. Mentions it could be helpful, could be beneficial.	I'd be okay/comfortable with that. That would be cool. I don't really have any objection.
Conflicted/Mixed	Could see both sides, expresses equal amounts comfort and discomfort, could personally experience benefits and downsides without emphasizing either over the other. Context-dependent. Contrasts two or more things, negative and positive balance.	I'd be uncomfortable with it, but would like it for X. I'm on the fence. It depends on...
Uncomfortable/oppose	Expresses discomfort, disagreement, negative feelings, concern. Points out potential problems. If they sympathize with positive, ratio was 1/3 or less. If they present a positive, seems like an afterthought (not emphasized). Qualified with Existence not okay. If they say Existence Okay, they express explicit negative feelings; otherwise label as Comfortable Condition for exceptional use case is very minor	I'd be uncomfortable with that. That's creepy. I wouldn't want it to. I don't see the point. I wouldn't use it, except in ...
Attitude Emergent Code	**Definition**	**Statement Examples**
Would Use	Mentions use case or says they would use it	I would use that for X. I'd love for {usage} to be a thing.
Would Not Use	Says they would not use it	I can't think of a use for it. I would not want that.
Existence Okay	Accepts other people using it or its existence despite their discomfort. NOT implied through "would use" or "comfortable" tag.	I would want it available to others. I could see how other people might use this. I'm not opposed to the technology itself.
Existence Not Okay	Objects to its use or existence	I don't think that data collection feature should exist.
Conditional	Provides condition for acceptance or use	So long as... Only if...
Theme Emergent Code	**Definition**	**Statement Examples**
Ability to Turn-off	Mentions ability to disable or turn off sensors or features	I want to be able to (manually) turn off this feature
Advertising	Mentions advertising or marketing	I wouldn't want to get ads while...
Amelioration	Improves quality of life for coping with disabilities.	It'd be helpful to me as someone with an ocular disorder/ADHD/autism/etc. This would be great for {condition}
Benefits Me	Says it would be useful, helpful, beneficial; provides utility	That would be useful for when I...
Bystanders	Considers situations, consent, or feelings of other people	I don't want it to record other people/my friends/my kids.
Collector Matters	Company or custodian of the data	It depends on who's getting my data. Do I trust the company?
Consent/Opt-in-out	Mentions consent or opting in/out	I want it to require my consent. I'd like the ability to opt-out.
Context/Situation Matters	Any situation (e.g., location, time) serving as a condition	Not in the home
Data Protection	Anonymization, encryption, PII revealed, secure storage	I wouldn't want my data to be tied back to me.
Data Use/Purpose	Concerns about how their data will be used: advertising, medical, product development, etc.	I'd be concerned about how they're using this data.
Data Retention Matters	Retention and deletion of data matters	I want to be able to delete or remove it
Some data off-limits/ Data Content Matters	What is collected (data content) or represented by the data matters.	It depends on what the data is (e.g., birthday, web history)
Discrimination	Unfair treatment, could exacerbate inequalities or social injustice	Employers could unfairly use this against me/others.
Initiated by User	Should occur only if user starts or requests it	Only if I start recording
I'm Used to It	Accustomed to data collection/usage as it already occurs on other devices.	I'm used to it. My phone already does this.
Legal Protection	Wants or imagines regulation compliance like HIPAA, GDPR, CCPA, etc.	I can't imagine that would be legal, given health laws.
Mental Health	Would have an effect on people's emotional and psychological well-being, ability to function in society, and meet the ordinary demands of everyday life.	I'd be worried about potentially worsening body dysmorphia or becoming over self-aware, addicted, or over-dependent.
Notice & Comprehension	Notification or some way to understand data policies is provided	I'd like to know what they're using my data for.
Personal Threat	Potential harm to person or property, e.g., theft, physical attack, identity theft	Data could be used by stalkers.
Recording	Whether device is recording, even for the short-term, affects how they feel.	I wouldn't want it to always be recording.
Storage Matters	Storage location of data. Local/device, personal cloud, company cloud	As long it's only stored locally on my device.
Third-party Access	Sharing data with third party companies, advertisers, employers	I don't want my employer to collect this data

D APPENDIX - DEMOGRAPHICS

Our screening survey included questions about age, gender[1], race or ethnicity[2], and income. During our interviews, we gathered background information about the AR technology (e.g., device or app) they used most often and their attitudes[3] regarding data collection for that AR technology. Current technologies included Hololens (version was not always specified), VR devices (including Oculus), Niantic mobile AR games Ingress, Pokémon GO, Harry Potter Wizards Unite (HPWU), and apps that use AR technology (PolyCam, Instagram, Snapchat, and Google/Apple Maps).

Age	Gender	Race	Latinx	Income	Recruitment Source	AR Device/App	Attitude
21	P	NL	No	Prefer not to respond	r-augmentedreality	Pokemon Go	C
31	M	W	No	$50-60k	r-hololens	VR Device	C
31	NL	W	No	$20-30k	r-pokemongo	Pokemon Go	C
30	M	W	No	$100-150k	r-ingress	None	M
58	F	W	No	$100-150k	r-ingress	Ingress/HPWU	M
24	NB	AS	No	$80-90k	r-ingress	PolyCam	C
25	F	AS	No	$20-30k	r-pokemongo	Pokemon Go	M
34	NB	AS	No	$20-30k	r-ingress	Oculus	C
33	F	W	No	Prefer not to respond	r-ingress	Pokemon Go	M
41	F	W, AS	No	Prefer not to respond	r-hpwu	Ingress	U
19	F	B	No	$60-70k	r-hpwu	Instagram	No Response
32	M	W	No	$100-150k	r-hpwu	HPWU	C
28	F	A	No	$100-150k	nml	Snapchat / Instagram	M
25	M	NL	No	$80-90k	r-ingress	Pokemon Go	C
31	M	W	No	$50-60k	r-pokemongo	Hololens	M
26	A,F,G,NL	NL	No	$10-20k	r-ingress	Hololens	M
27	M	W	No	$100-150k	r-augmentedreality	Hololens	C
27	M	W	No	$100-150k	r-augmentedreality	Hololens	M
24	M	W	No	$50-60k	r-hololens	Hololens	M
38	M	W	No	$100-150k	r-hololens	Hololens	U
46	M	W	No	$100-150k	r-hololens	Google/Apple Maps	C

[1]Gender: F=Female, M = Male, NB = Nonbinary, NL = Not Listed above,
P = Prefer not to respond, A = Agender, G = Genderqueer
[2]Race/ethnicity: AA = African American/Black, AS = Asian,
H = Hispanic/Latino/Latina/Latinx, W = White, NL = Not Listed
[3]Attitude: U: Uncomfortable/Opposed, M: Mixed/Conflicted,
C: Comfortable/support