Don't Record My Private pARts: Understanding The Role of Sensitive Contexts and Privacy Perceptions in Influencing Attitudes Towards Everyday Augmented Reality Sensor Usage

Melvin Abraham* Mohamed Khamis† Mark McGill‡

University of Glasgow

ABSTRACT

Everyday Augmented Reality (AR) headsets come with an array of sensing capabilities. Users wearing these headsets for extended periods may prefer specific sensors to remain inactive in some contexts for privacy and sensitivity reasons. Currently, the contexts in which users wish to limit sensor data collection are unclear. To explore this, we conducted a survey (N=100), collecting 552 scenarios to understand which situations users wish to restrict or completely block data collection by specific sensors or combinations on their AR headset. Our results show the sensitive contexts can be classified into seven categories: 1) presence of confidential information; 2) risk of data quantification; 3) expectation of solitude; 4) rules prohibiting data collection; 5) modesty and nudity; 6) home environments; and 7) outdoor public locations. Our results provide insights into privacy-invasive contexts when people want to limit and restrict their AR sensors, building towards automating permission configurations during the prolonged use of everyday AR headsets.

Index Terms: Augmented reality, data access, permissions, context, location, privacy, access control, sensitive contexts.

1 INTRODUCTION

Augmented Reality (AR) headsets are seeing an increase in adoption [5, 23, 45–47, 68], with advances in spatial computing leading to devices being designed to be more fashion-forward and practical to wear throughout the day, such as AR glasses [12, 30, 55]. It is anticipated that in-time, *Everyday AR* headsets will be worn for long periods throughout the day, complete with 'always-on', requisite sensing [55] that drives their ability to understand and augment our perception of the world [2, 12, 30, 55, 59, 60]. AR headsets are equipped with a number of sensors and can sense a large quantity of data about the user [2, 17]. Attributes such as the user's body position, depth information of objects in their vicinity, a view of their surroundings, and voice recognition of nearby speech can be collected onboard the headset [17, 26]. Further data that users may be less aware of can also be collected and combined to infer other information [2, 17], such as the user's visual interests using built-in eye tracking [2] or emotions using behavioural data [2, 25, 50, 59].

Most AR devices today are based on the Android operating system [1,22,48], and the current method to control what data an application can access is via permissions [22, 67]. Permissions in most AR platforms are currently set once by the user and will not change until the user goes out of their way to reconfigure them [15, 22, 67]. Nevertheless, literature shows users tend not to alter their permissions at a later point after granting access [39, 41, 63, 67], or even worse that people can quickly forget they are recording despite being reminded [71]. As everyday AR headsets are meant to be worn in different locations and contexts [60], situations will arise where AR users would want to limit or restrict their AR headset's data collection. Hence, there is a need for AR permission systems to handle dynamic changes in data access based on the context without explicit user involvement.

To address this gap in understanding how the acceptability of everyday AR sensing might vary throughout the day in different contexts, we conducted a survey (n = 100) to gather descriptions of locations and scenarios (n = 552) of prospective AR usage that people classed as privacy-sensitive. We then generalise the contexts by categorising their attributes into *sensitive context archetypes*. The archetypes are accompanied by a list of AR sensors our participants would like to be restricted or limited within those contexts.

1.1 Contribution

We provide empirical evidence on two aspects of AR sensing data collection: the influence of contextual factors beyond location, and the specific impact of different sensors within those contexts. First, we show that the broader contextual environments we categorise into seven sensitive context archetypes affect the perceived appropriateness of collecting AR sensing data e.g. while participants generally express low concern about the use of front cameras, they become significantly more concerned in contexts involving nudity or within home environments. Second, we show that perceptions towards the appropriateness of AR sensing are significantly impacted by the type of sensor involved and the context in which data is being collected e.g. our participants are significantly more concerned about microphone data than body-sensing data in contexts where confidential information may be present, such as a financial building or a healthcare centre. We make the following contributions:

1. We report results from a survey collecting perceived sensitive locations and scenarios and where respondents desire to limit or restrict their AR headset's data collection across one or more sensors;
2. Based on the above, we derive sensitive context archetypes that describe the underlying reasons behind *why* said contexts are perceived as sensitive by respondents;
3. For each sensitive context archetype, we report initial recommendations regarding *what* sensors drive respondent concerns and should be considered to be restricted or at the very least limited on an Everyday AR device.

We see our work as a necessary step towards automated permissions that ensure a base level of privacy that is appropriate for the different contexts of an Everyday AR user.

2 RELATED WORK

Previous work has looked at limiting data access using OS-level data abstractions called recognisers to enable AR fine-grained permissions [29]. Roesner *et al.* [60] used these recognisers [29] to build a world-based access control that changes permission access

*e-mail: m.abraham.1@research.gla.ac.uk

†e-mail:mohamed.khamis@glasgow.ac.uk

‡e-mail:mark.mcgill@glasgow.ac.uk

levels when the user is in a sensitive location [60]. A missing element is an empirical list of where those sensitive locations are. Moreover, Schmidt *et al.* [61] showed that location is only one factor of many to form a complete context. Location alone is insufficient to describe what contributes to making locations sensitive in an actionable way and what specific sensors should be restricted or limited, hence the need to investigate sensitive contexts. Abraham *et al.* [1] studied how users could provide less than full AR data access by introducing a new fine-grained permission system explicitly designed for everyday AR headsets. The proposed permission systems allowed AR users options to provide variable data access and fidelity levels for varying application functionality. Users could appropriately balance their privacy and user experience by being provided with an image of what the application would look like at a chosen level of data access. Abraham *et al.* [1] suggest that future AR headsets should move towards automating the permission configuration process based on baseline permissions settings, previous permission behaviours, and the user's context to prevent burdening the user from manually changing their permissions when they are in a new location or situation [1]. Similarly, Hoyle *et al.* [27] analysed the privacy concerns of '*lifeloggers*' using wearable cameras, and focused on what makes photos private and their participant's preferences when it came to sharing the photos. They found that Lifelogging photos often capture private moments which tend not to be typically photographed, such as personal documents or intimate settings [27]. Hoyle *et al.* highlighted the need for automated tools that detect, manage and curate lifelogging images to prevent accidental privacy leaks. Similarly to Roesner *et al.*, [60], a list of sensitive contexts suggesting when to limit data collection and which sensors specifically need to be limited is missing. Furthermore, the permission system still places the responsibility of reconfiguring the permission settings on the user. while previous work has shown that users tend to not go back and change their permissions after initial configurations [39, 41, 63, 67] or even forget they are recording even when reminded [71]

2.1 Camera Access Controls

When looking at restricting specific sensors, prior literature has looked at how to stop AR headsets from recording sensitive front-camera footage [7, 28, 66]. In foundational work around privacy and AR, Koelle *et al.* [32] conducted a focus group with seven participants to explore what situations the usage of "*data glasses*" are inappropriate or can be controversial. Their work presented a list of nine controversial situations, such as "*when children are involved*" or "*walking in urban areas*" [32]. Koelle *et al.* also listed five controversial application types such as "*navigation*", "*reading news, messages*", and "*gaming*" [32]. While their work provides a valuable general overview, it also highlights areas for future research, such as the specifics of actual locations and which sensors should be limited or restricted in those situations. Steil *et al.* [66] recruited seventeen participants to wear smart glasses to record their point of view through a front-facing camera. Participants then coded the footage to state when sensitive moments were captured. The coded data was used to train a machine learning model to identify potentially sensitive situations and close a physical shutter in front of the camera [66]. While this innovative approach is a step forward, we advance it further by a) investigating which sensors, other than the front camera, might require similar restrictions, and b) considering the necessity of sensors that are required to deliver AR.

2.2 Risks to Bystanders

Wolf *et al.* [70] argued that considerable attention had been provided to prevent '*always-on*' front RGB cameras from capturing video of the user and bystanders without proper consent [7, 28, 31, 42, 66]. However, prior work has given significantly less attention to protecting users from being sensed by the other '*always-on*' sensors on the headset, e.g. auditory input [70] or eye-tracking [9] and suggests that future work should look at methods that allow '*always-on*' sensors to be active conditionally. Denning *et al.*, [10] conducted '*in-the-wild*' sessions and interviewed thirty-one participants in a cafe to look at bystander perspectives when co-located with an AR user potentially recording audiovisual data. Participants listed some factors that made them feel unsafe or that their privacy was being invaded, such as the ease of being recorded without the bystander's knowledge or what the AR user will and can do with the footage [10]. Denning *et al.* also provide nine design axes for privacy-mediating technologies based on participant concerns. Denning *et al.*'s work was one of the first to collect real-world perspectives on a bystander's view of AR audiovisual data being collected. Our work builds on this by looking at the AR users' perspectives of multiple sensors and goes beyond only the front camera and microphone. O'Hagan *et al.* [55] also looked at AR bystander privacy preferences by conducting a survey. This work discusses examples of situations participants found inappropriate for AR headsets to be collecting data. Our work extends this by a) investigating the appropriateness of specific active sensors within sensitive context archetypes, and b) what baseline preferences participants have for multiple everyday AR sensor data collection.

Lee *et al.* [36] surveyed 1,782 people to identify the most concerning scenarios about data disclosure from wearable devices. In the survey, their participants were mostly concerned about photos containing personal or embarrassing content, nudity, or financial information being shared with others [36]. The participants stated they would be much more upset if their data was shared with other people, especially people they know personally, compared to being shared with other applications or stored in a server [36]. The same sentiment was shared when participants stated they were less concerned by their data being collected and inferred, similar to if they were observed in public, such as demographics [36]. And Lebeck *et al.* [35] conducted a qualitative lab study with 22 participants using the Microsoft HoloLens to explore security, privacy, and safety concerns. Lebeck *et al.* stated that AR devices would be used around other users and not in isolation hence uncovering unique security and privacy concerns. Examples include deceptive virtual objects, placing virtual objects in each other's faces or attempting to control shared objects [35]. Lebeck *et al.* recommended the need for a new AR access control specifically for shared spaces [35].

3 Study Design and Methodology

A survey was conducted to capture privacy-sensitive locations and scenarios while wearing an AR headset and subsequently determine which sensors participants would want to limit or restrict in those locations. The locations were grouped into sensitive context archetypes based on the scenario. The survey involved participants being onboarded to what AR is and the sensing capabilities of AR headsets (see section 7). The survey captured a baseline of how appropriate a specific data type is to collect in general, irrespective of any context. Then, participants were asked three times to provide a privacy-sensitive location with the option to provide more. For each location provided, details about why they perceived that location to be privacy-sensitive and the appropriateness of the same data types being collected were asked.

As privacy is considered personal and contextual [43, 53, 54], we asked participants to provide their own privacy-sensitive locations. Doing so allowed us to build on the work by Koelle *et al.* [32], which investigated controversial situations while wearing "*data glasses*" to see if any context or locations have changed, evolved or generalised since their study in 2015. We define privacy-sensitive as "*a situation in which you would like to be kept secret and potentially private from other people or things*". Our IRB granted ethical approval before any research was conducted. The survey took 10-15 minutes to complete. The final data set was made up of 100

participants and collected 552 scenarios with a mean of 5.52 (*Mdn* = 6, and *SD* = 2.67) scenarios reported per participant.

3.1 Sensors and Data Types

We compiled a list of sensors from both previous work [17,24] and the technical specifications of the Microsoft HoloLens 2 [26], the Varjo Aero [4], and Meta Quest Pro [49] whose sensing capabilities could find their way into everyday AR headsets. Our list of sensors is not exhaustive; nonetheless, it is representative of what is feasible in existing consumer XR devices. When presenting the questions to the participants, we refer to the sensors as a description of the raw data they collected in layperson's terms to increase the quality of the responses if participants were unaware of what a sensor is or what it collects. Previous work suggested that participants struggle to understand the concept of privacy-sensitivity and recommend asking for the appropriateness of the sensor being active [66]. See Table 1 for the data type descriptions and sensor pairings.

3.2 Recruitment and Demographics

Initially, we received 469 responses and filtered out 369 responses from the survey due to fraudulent entries such as spam, bots, or failing the attention check question, as many bots and scams exist to farm monetary rewards for completing questionnaires [56]. Most of the bots and spam were flagged by Qualtrics [58], via the '*Expert Review Fraud Detection*' using features such as flagging known spam bot IPs and implementing a reCAPTCHA [57]. For the check question, on the same page when the participant was entering the 2nd location and scenario we asked the participants to select "*Strongly agree*" to show they are paying attention. All of the responses which did not select "*Strongly agree*" for this question were removed. From the 369 removed responses, 189 of them failed the attention check. Additionally, non-English posts, responses that made no sense, or responses that were clearly generative AI and did not make sense within the context of the question were omitted manually, after being agreed upon by 2 or more co-authors. Once we removed all the fraudulent entries, the final data set was comprised of 100 complete responses and 552 scenarios.

The mean number of scenarios per response was 5.52 (*Mdn* = 6, and *SD* = 2.67). We advertised on X/Twitter with the hashtags "*#AR*" and "*#privacy*", mailing lists, and the *r/VisionPro* and *r/SampleSize* Reddit forums. Participants could enter a prize draw to win one of five £10 Amazon vouchers. Only participants aged 18+ could take part in the survey. The participants' ages ranged from 18-73 (*M* = 31.7, *SD* = 9.82). 42 participants self-identified as female, and 58 self-identified as male. The option of non-binary and other was available, but it was not selected. For participants AR experience 3 claimed they have never heard of AR, 20 claimed they have never used AR but know of it, 37 claimed they have used mobile AR infrequently (e.g. AR games such as Pokemon GO), 17 claimed to have used mobile AR frequently, and 23 claimed they have used an AR headset (Hololens, VR headset with passthrough).We received responses from 14 countries, with 55 participants from the UK. The majority of the participants were from Europe, making up 63% of the dataset, followed by North America 28%, Africa 4%, Asia 2%, and Oceania 3%.

Table 1: Sensors and their data type descriptions

Sensor	**How appropriate is it that, in this scenario, your headset has access to...**
Body and IMU e.g sensors, gyroscope	your head and body's orientation?
Depth and LiDAR sensors	depth and distances of surfaces and objects around you?
EEG sensors	your brain activity?
Eye Tracker	what you are looking at and your eye-movements?
Front facing RGB-camera	a view of your surroundings in full colour?
GPS	your precise location?
Microphone	the audio from you and your surroundings

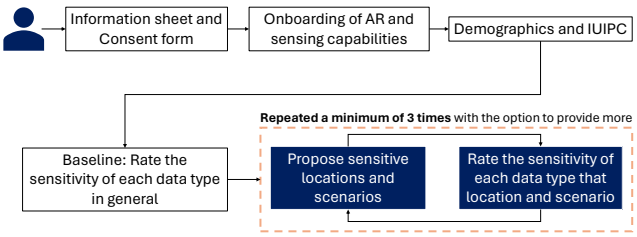

Figure 1: The survey is comprised of 5 sections. 1) Reading an information sheet and consent form. 2) Being onboarded to what AR is, the sensors, and the sensing capabilities. 3) Providing demographic information and the IUIPC [40]. 4) Providing the appropriateness and sensitivity of the data types in Table 1 in general, irrespective of context, to form a baseline. 5) Propose at least 3 privacy-sensitive locations and scenarios with the opportunity to provide more and then rate the sensitivity of the data types in Table 1 within that scenario. The full procedure can be read in subsection 3.3, and the complete survey can be accessed in section 7.

True everyday AR, in which most of society uses AR headsets continuously for prolonged periods, does not yet exist. This work identifies and protects users from privacy issues before they become a reality. Hence, we included participants from all backgrounds and experiences with AR, including participants who had never used or heard of AR before. The rationale for including participants with little to no AR experience was that they currently do not use AR; however, these same people will be impacted in the future. Thus, their views are still considered valid and important. We provide an onboarding stage to every participant (see section 7) to explain what AR is, the idea of everyday AR, the sensors equipped on AR headsets, and a general description of what the sensors can collect. The onboarding stage ensured that all participants had the required baseline level of AR knowledge before starting the questionnaire, thus supporting the validity of the results.

The participants' general privacy attitudes were gauged using the *Internet Users' Information Privacy Concerns questionnaire* (IUIPC) [40]. The IUIPC's score is between 1 which represents a low privacy attitude and 7 represents a high privacy attitude. Participants rated their wish for control (M = 5.85, SD = 1.23), awareness (M = 5.78, SD = 1.34), and the perceived ratio between benefit and collection (M = 5.57, SD = 1.30). Note that a limitation of privacy questionnaires is that they only provide a *theoretical* view of a user's privacy attitudes and do not provide insight into if the attitudes are present in practice [19]. Nonetheless, the mean scores implying the participants represent a high general privacy attitude.

3.3 Procedure and Measures

The complete survey is presented in section 7, and an overview of the survey can be seen in Figure 1. The survey started with gathering informed consent. Participants were then on-boarded into what everyday AR is and a description of the sensing capabilities of the headset; see section 7 for details. Once the survey began, participants were asked to complete a demographic form about their AR experience and the IUIPC privacy attitudes questionnaire [40]. Next, participants were asked to "*Place yourself in a future where people commonly wear and use AR headsets in their*

everyday life, similar to smartphones today". Baseline questions of general appropriateness of data types were asked as presented in subsection 3.1 using a 5-point scale (1=Very inappropriate;5=Very appropriate) irrespective of context. Participants were given a free text box to explain why they rated any statements as "*Very inappropriate*" or "*Somewhat inappropriate*". Next, participants were asked to explain any concerns regarding wearing a device with access to all the above data types, if any.

Participants were introduced to privacy-sensitive locations and asked to provide a location. Next, participants were asked to provide a privacy-sensitive scenario within their provided location. Then, they were asked how comfortable they are that data from this scenario is collected and shared with others via the same 5-point scale used earlier for the baseline and free text to provide a rationale. Finally, participants were asked about the appropriateness of data types from subsection 3.1 being collected in this location. Participants repeated this section twice and were allowed to provide more locations. An attention check was added to ensure the participant's focus. The complete survey is presented in section 7.

3.4 Analysis

3.4.1 Influence of Context on Appropriateness

Bots identified through Qualtrics and failed attention checks were removed. The respondents' ratings of the appropriateness of data types in all sensitive locations were compared to their baseline ratings by grouping all the sensitive locations to see if there was a location and sensor that had an effect. As our data was non-parametric [62, 69], an Aligned-Rank Transformation (ART) [13, 69] was applied to the dataset using ARTool [14], and then a one-way repeated measures ANOVA was conducted. As the differences were significant ($F(1) = 687.42$, $p < 0.001$; $\eta_p^2 = 0.08$), this motivated looking at the specific locations (See Figure 2 for the mean appropriateness scores for each of the sensors between the baseline and all the sensitive locations combined and section 7 for the full pairwise comparisons). Hence, inductive coding [44] was used to analyse the locations within the responses. One researcher iteratively coded all the sensitive locations based on similarities of the locations (e.g., hospital building, hospital, and doctor's office were coded as HealthcareCentre). Once the initial location codes were formed, the lead and secondary researchers reviewed and discussed the codes after another iteration the final codebook was formed (see section 7).

3.4.2 Sensitive Context Archetypes Formation

The lead researcher thematically grouped the codes into sensitive context archetypes. The archetypes emerged through patterns and similarities based on the scenarios provided by the participants. Hence, some locations appear in more than one archetype. To form the final codebook, iterative reviews and discussions by the lead and secondary researchers were carried out over collaborative sessions, during which all locations and archetypes were examined. The final codebook of archetypes and their locations can be seen in section 7. As the final archetypes had different numbers of entries, the data was bootstrapped [6, 11, 37] to 328 re-samples with replacement so fair comparisons could be made statistically. 328 was chosen as this was the highest number of responses for an archetype before bootstrapping. Bootstrapping the dataset was appropriate as the data follows a non-normal distribution, and the number of responses per location was unbalanced [6, 11]. From this, another ART was performed, and a one-way ANOVA was conducted on the sensor appropriateness across each sensitive context archetype. The partial eta-squared test (η_p^2) score was used to report effect sizes. The effect size was small when $0.01 \geq \eta_p^2 < 0.06$, medium when $0.06 \geq \eta_p^2 < 0.14$, and large when $\eta_p^2 \geq 0.14$ [16, 51]. The full pairwise comparisons can be found in section 7.

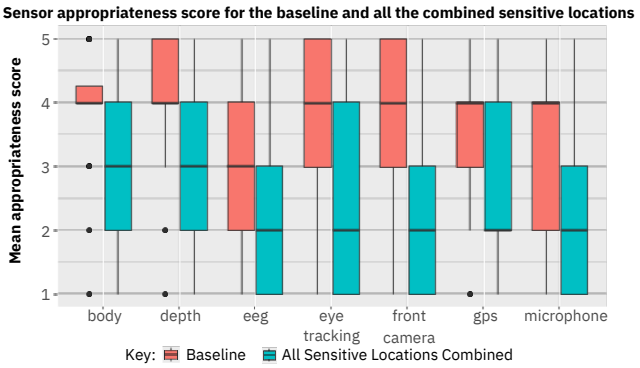

Figure 2: Plotted on a boxplot is the mean appropriateness score of each of the sensors being active for the baseline compared to the mean appropriateness score of each of the sensors being active within all the sensitive locations combined together. 5-point Likert scales 1 = Extremely inappropriate to 5 = Extremely appropriate. The boxplot shows that within any sensitive location, all sensors are scored as less appropriate to be active compared to the baseline scores. This shows that further investigation is needed into the sensitive locations themselves to know what contributes to the locations being considered as sensitive in the first place.

3.5 Limitations

The size and demographics of our sample of respondents mean that our results are formative and cannot speak to geographic or cultural differences around the perceptions of AR sensing. The UK had the highest representation with 55 out of 100 participants, followed by the USA with 28. Both countries were responsible for 83% of the total responses. Thus demographic spread of our results is illustrative of a bias towards English-speaking countries. Additionally, the survey was posted on Reddit, X/Twitter, and mailing lists, so our participants are likely to come from a pool of individuals who are willing to try new technologies (e.g., gamers and technology enthusiasts) as well as the pool of potential participants would be limited to countries where those websites were not banned/blocked. Future work would benefit from taking a cross-cultural perspective on sensitive context archetypes. Moreover, the 7 sensitive context archetypes we present are not a complete list of all possible sensitive context archetypes, but rather a representation of recurring themes in our responses. Nevertheless, this work provides the first empirical evidence on how sensitive contexts influence attitudes towards multiple everyday AR sensor usage, and highlight the existence and predominant types of sensitive context archetypes where people may desire to restrict AR headset data collection.

4 Results

Here we present seven sensitive context archetypes. Sensitive Context Archetypes refer to the attributes that contribute towards a context becoming private. See Table 2 for a summary of the archetypes.

The Sensitive Context Archetypes and sensor means, standard deviations, statistical difference, effect size, and pairwise comparisons can be seen in Table 3. The qualitative results for each archetype is presented below. For each sensitive context archetype, all reported locations are presented with the full list in section 7.

4.1 Modesty and Nudity

4.1.1 Locations and Perceived Sensitivity

This sensitive context archetype has 10 locations, with 328 responses. The location with the most occurrences was the *bathroom* with 142 occurrences. Activities that are "*are super private and sensitive.*" (P71) such as "*Going to the toilet*" (P70), "*Have a bath*"

Table 2: The sensitive context archetypes presented in order of most responses to least. The *Modesty/Undress* sensitive context archetype has the highest number of responses, *Home* was second, and *Presence of Confidential Information* was third.

Sensitive Context Archetypes	Description/Rationale	# of Locations	# of Responses
Modesty/Undress	A state when users or those around them are wearing little to no clothes	10	328
Home	Location in a home or a place people live	9	298
Presence of Confidential Information	In a situation where information that is private, sensitive or confidential is present both written or said.	15	209
Rules Prohibiting Data Collection	A situation where an authority prohibits the collection of data (e.g., not allowing cameras in a cinema)	11	163
Risk of Data Quantification	In a location where users do not want what they are doing or the things around them tracked and collected	9	78
Expectation of Solitude	A situation where you expect to be alone or without technology	5	37
Outdoor Public Location	Location that is outside	5	39

(P42), or "*taking a shower in the toilet*" (P71) which could "*be really embarrassing*" (P82) if captured. P64 went to mention considerations based on sex need to be taken into account, "*As a woman, when taking a bath and changing clothes in the bathroom, I am afraid that the private parts of the body will be photographed and leaked*". A similar point was shared by P66 "*if leaked these info could lead to blackmail or cyberbullism*".

The bedroom was another location that was reported 71 times. P4 brought up "*I could imagine a situation where, for example, I would forget I was wearing an AR headset or leave my AR headset in a private space where I might then engage in private activity (e.g. getting dressed or changed, having a sensitive conversation with someone) without realising my headset was capturing data*". Participants stated vulnerable moments could be captured, such as "*being intimate with your partner*" (P66), "*Getting undressed*" (P70), and "*Any moments of shared intimacy*" (P3). Consequences of such personal information being collected such as "*Both visual, audio (and potentially the location) aspects of the situation can put the user in a vulnerable state* " (P3). P4 went on to say, "*I believe that would be a blatant invasion of privacy, and I'm uncomfortable with how easily it might occur, even by accident*".

A Locker changing room was mentioned 9 times. P79 mentioned, "*This would be a violation of privacy particularly for the people around me using these facilities who of course would not want this being captured by an AR device*". P3 shared a similar opinion of "*All kinds of personal information mine and other people's would be captured, nudity in particular*".

4.1.2 Sensors and Appropriateness

None of the sensors were rated as appropriate to be active, with *front facing camera* (M = 2.17, SD = 1.43), and *microphone* (M = 2.19, SD = 1.24) rated as least appropriate to be active.

4.2 Home Environment

4.2.1 Locations and Perceived Sensitivity

This sensitive context archetype has 9 locations, with 298 responses. 50 participants stated their house was a sensitive location as "*It no longer just affects me but now my family*" (P10). P7 stated "*It's an intimate moment, and a situation where myself and my partner can just be ourselves, I don't want corporations to figure out how to monetize my relationship behaviour*". Other personal information can also be captured within a home as stated by P63 "*overheard conversations or phone calls*" or "*Viewing personal documents, viewing inside the home*" as stated by P12. P69 stated they would like to keep their home private as a matter of personal safety "*Someone could get information about the layout of my home and break in and steal. They would know if I was at home or not and could rob if empty or attack if I'm there*".

Specific areas within the home such as *the living room* were mentioned as participants may be engaging in "Private conversations with family / friends. Access to online services (banking, shopping, etc.). Looking at personal documents" (P68). A point shared by P79 "*I could be having personal or intimate conversations or moments which I would not want other people to see. This could include speaking to family or romantic partners about difficult and private subjects*". Outside of the participant's permanent home, temporary accommodations such as "*Hotels*" (P34) or "*Carehomes*" (P81) were also mentioned.

Other people's homes were also brought up as a sensitive location such as "*In the home of somebody I know (family, friends)*" (P72) or "*Attending a dinner party*" (P1). P1 stated that "*It is no longer within my personal space, it is in other people's personal space*". P92 mentioned that "*the main risk here is reputational damage or a breakdown in a relationship*". Due to "*I would rather not want to share data from their houses*" as P72 stated.

4.2.2 Sensors and Appropriateness

No sensors were rated as appropriate to be active, with *front facing camera* (M = 2.34, SD = 1.39), *microphone* (M = 2.36, SD = 1.32), and *EEG* (M = 2.36, SD = 1.35) rated as the least appropriate.

4.3 Presence of Confidential Information

4.3.1 Locations and Perceived Sensitivity

This sensitive context archetype has 15 locations, with 209 responses. The location with the most occurrences was *a place of work* with 69 occurrences. P8 stated that "*In meetings with sensitive topics, or regarding proprietary work that should not be shared outside*". P6 said they talk to "*colleagues with whom I share a very professional relationship and I wouldn't appreciate disclosing my personal information to professional life colleagues. Would appreciate having boundaries*". A few participants mentioned other types besides conversations could be captured such as "*"Work information that the company wouldn't want to be shared. (Passwords, methods etc)*" (P85); "*You can capture whats on screens; the inputs (official, notes) Depending on the type of work you do this may pose many issues (Data loss prevention team / HR / finance)*" (P96); or "*Floor layout, staff listing, itinerary listings*" (P96).

P96 went on to share "*The office peers around me have differing levels of security access and permissions to view different data, tools and topics; hot desking makes it harder to create secure spaces for teams to enforce a level of control. So you could potentially be capturing various sensitive data from a variety of spaces ordinarily ignored by a glance and captured by the AR tech*".

Healthcare Centres were reported 42 times. P33 stated "*You may be discussing a personal health issue with your doctor, which is a private medical consultation*". P4 stated that collecting just being at

Table 3: Statistical testing for the sensor appropriateness score (1=Very Inappropriate, 5=Very appropriate), Means and SDs by sensitive context archetypes and Sensor, including *post hoc* significant pairwise comparisons using ART-C [13] with Tukey corrections. Cells in green highlight rows with a significant main effect. A heatmap on the mean (standard deviation) ranges from purple (Very Inappropriate) to white (Very appropriate) based on the 5pt Likert scale. The η_p^2 heatmap ranges from white (0.01, small effect size) to blue (0.14, large effect size).

Archetype / Sensor	**1. Body**	**2. Depth**	**3. EEG**	**4. Eye-Tracking**	**5. Front-Camera**	**6. GPS**	**7. Micro-phone**	**ANOVA**	η_p^2	**Pairwise Sensor Comparisons**
Modesty and Nudity	2.87 (1.49)	2.88 (1.38)	2.46 (1.38)	2.45 (1.36)	2.17 (1.43)	2.79 (1.31)	2.19 (1.24)	$p < .001$	0.05	(1 - 3), (1 - 4), (1 - 5), (1 - 6), (1 - 7), (2 - 3), (2 - 4), (2 - 5), (2 - 6), (2 - 7), (3 - 7), (4 - 7), (6 - 7)
Home Environment	3.11 (1.44)	3.01 (1.39)	2.36 (1.35)	2.67 (1.45)	2.34 (1.39)	2.81 (1.31)	2.36 (1.32)	$p < .001$	0.05	(1 - 3), (1 - 4), (1 - 6), (1 - 7), (2 - 5), (2 - 6), (2 - 7), (3 - 5), (3 - 7), (4 - 5), (4 - 7), (5 - 6), (6 - 7)
Confidential Information	3.23 (1.31)	3.10 (1.26)	2.42 (1.26)	2.28 (1.22)	2.03 (1.17)	2.42 (1.20)	1.86 (1.18)	$p < .001$	0.15	(1 - 3), (1 - 5), (1 - 7), (2 - 3), (2 - 5), (2 - 6), (2 - 7)
Rules Prohibiting Data Collection	3.38 (1.42)	3.16 (1.40)	2.37 (1.17)	2.26 (1.31)	1.97 (1.21)	2.56 (1.18)	1.99 (1.27)	$p < .001$	0.15	(1 - 5), (1 - 7), (2 - 3), (2 - 4), (2 - 5), (2 - 7), (3 - 5), (3 - 7), (4 - 5), (4 - 7), (5 - 6), (6 - 7)
Risk of Data Quantification	2.37 (1.27)	2.38 (1.16)	2.25 (1.09)	1.82 (0.95)	1.78 (1.10)	2.31 (0.96)	1.63 (0.96)	$p < .001$	0.11	(1 - 5), (2 - 3), (2 - 5), (2 - 7), (5 - 6)
Expectation of Solitude	2.97 (1.39)	2.59 (1.17)	2.19 (1.17)	2.42 (1.33)	2.41 (1.51)	2.55 (1.08)	2.25 (1.14)	$p < .001$	0.04	(1 - 6)
Outdoor Public Location	2.66 (1.43)	2.50 (1.32)	2.75 (1.41)	2.23 (1.33)	2.14 (1.34)	2.41 (1.26)	2.24 (1.29)	$p < .001$	0.03	(1 - 4), (1 - 5), (1 - 7), (2 - 5), (3 - 4), (3 - 5), (3 - 7), (5 - 6)
Baseline	3.90 (1.01)	4.22 (0.98)	2.93 (1.43)	3.48 (1.32)	3.74 (1.23)	3.67 (1.08)	3.28 (1.24)	$p < .001$	0.11	(1 - 7), (2 - 3), (2 - 6), (2 - 7), (4 - 7), (5 - 7)

a medical building is highly sensitive "*receiving a sensitive diagnosis, being geotracked (e.g. someone visiting a fertility or abortion clinic)* ". P4 then said that "*Medical information is very confidential and private (hence the focus on doctor-patient confidentiality in many fields), and I would be uncomfortable with unknown actors receiving information on this. You could imagine a life insurance plan being cancelled in the wake of a cancer diagnosis or similar*".

Financial buildings were reported 5 times. P11 mentioned the large quantity of personal information that is present as "*Discussions with bank staff will contain information about your financial situation as well as private information such as DoB, address, NI number etc* ". P2 stated "*A conversation between a client and a financial advisor about a financial plan for a business.*" shows the level of confidentially needed at the early stages of entrepreneurship. P92 mentioned "*perhaps an ongoing court case, perhaps an upcoming surgery, perhaps a failed mortgage bid*". P92 then said "*because this information is not only potentially embarrassing if leaked, it could have serious professional or personal implications. All of the above might affect prospects of being hired or promoted, impact personal or professional relationships, or impact the availability of further medical, legal or financial options going forward*".

4.3.2 Sensors and Appropriateness

For all quantitative results see Table 3. None of the sensors were rated as appropriate, with the*microphone* (M = 1.86, SD = 1.18), *front facing camera* (M = 2.03, SD = 1.17), and *eye-tracking* (M = 2.28, SD = 1.22) being rated least appropriate to be active.

4.4 Rules Prohibiting Data Collection

4.4.1 Locations and Perceived Sensitivity

This sensitive context archetype has 11 locations, with 163 responses. The location with the most occurrences was *a spa* with 6 occurrences. P70 stated "*I believe this would be a space that one would not necessarily wish to be recorded*". P54 mentioned a movie theatre or playhouse as a location with rules on recording "*It is not allowed to record in these scenarios so would not want to get in trouble*". P87 brought up that when in the "*presence of children ... it should be clear when the headset was active and recording data*". P34 mentioned police stations would prohibit recording information during "*During detention*".

4.4.2 Sensors and Appropriateness

None of the sensors were rated as appropriate to be active, with the *front facing camera* (M = 1.97, SD = 1.21) and *microphone* (M = 1.27) rated as the least appropriate to be active.

4.5 Risk of Data Quantification

4.5.1 Locations and Perceived Sensitivity

This sensitive context archetype has 9 locations, with 78 responses. The location with the most occurrences was *at a shop* with 5 occurrences. P65 stated, "*I don't want people to know my buying pattern*". P21 shared "*can reveal private information when shopping*". Participants also mentioned risks of "*identify theft"* (P69) as "*could get information like card and pin numbers*" (P69) or "*My password may have been compromised during payment*" (P20).

Social food venues were reported 7 times. P31 mentioned, "*AR headsets may record diners' conversations, orders, and possibly private chats and food preferences*". P13 brought up "*I don't like the idea of my AR glasses identifying what kind of fridge I have, what it contains and what kind of food I eat. This could be valuable information for advertisers*". Participants also stated how such locations allow AR headsets to "*film people without consent*" (P63).

Another perspective provided by the participants were based around the reason or intent of why the individual is in a location such as "*Elder people living in these homes for the elderly are typically in a vulnerable position and don't have the capacity to decide what they want to do with their data. They can also be easily influenced and manipulated.*" (P81). Another example provided by P97 was if the individual was at a "*protest*" as the headsets data could be collected and "*be utilized in a negative way*" i.g. using the headsets sensors to profile other protesters.

4.5.2 Sensors and Appropriateness

No sensors were rated as appropriate to be active, with the *microphone* ($M = 1.63$, $SD = 0.96$),*front facing camera* ($M = 1.78$, $SD = 1.10$), and *eye-tracking* ($M = 1.82$, $SD = 0.95$) least appropriate.

4.6 Expectation of Solitude

4.6.1 Locations and Perceived Sensitivity

This sensitive context archetype has 5 locations, with 37 responses. The location with the most occurrences (17) was *an educational establishment*. P10 stated, "*Feel I am exposing others to my process of learning, feel weird and vulnerable about it* ". P68 mentioned, "*Students may discuss problems or ask questions they'd rather not publicise, especially before or after session.*". A location that was mentioned once was a *place of worship*. P10 "*It feels that it breaks the connection between the faith and the individual (me)*".

4.6.2 Sensors and Appropriateness

None of the sensors were rated as appropriate to be active, with the *EEG* ($M = 2.19$, $SD = 1.17$), and *microphone* ($M = 2.24$, $SD = 1.14$) rated as least appropriate.

4.7 Outdoor Public Location

4.7.1 Locations and Perceived Sensitivity

This sensitive context archetype has 5 locations, with 39 responses. Being outside in a generic public location was mentioned 22 times. P8 mentioned "*If there is a social media aspect which is tracking your location and sharing it with others (perhaps a game like Pokemon Go), it could show other people when you are leaving your house empty, or allowing people to stalk you*". P14 stated data collecting in locations such as "*A park*" affects more than themselves as "*All the random people around me didn't consent*". P62 similarly stated, "*It makes others feel uncomfortable*".

Public locations such as "*Public transportation*" (P18) were also reported. P6 mentioned "*When using public transport, I would [not] prefer to share or allow anything to collect/store my precise location and travelling history in any way. I feel location history is a big threat*". P17 stated that if they were engaging in activities "*Like calling or messaging someone while on a public transportation*" then "*the data should only be shared to the one you are talking to as if they're receiving it, and not to the AR Headset as it doesn't need to process anything on that following data*". A beach was reported once by P17 as "*capturing other people on the beach*" can reveal "*super private and sensitive information*".

4.7.2 Sensors and Appropriateness

No sensors were rated as appropriate, with the *front facing camera* ($M = 2.14$, $SD = 1.34$), *eye-tracking* ($M = 2.23$, $SD = 1.33$), and *microphone* ($M = 2.24$, $SD = 1.29$) rated as the least appropriate.

5 Discussion and Future Work

We present seven unique archetypes derived from 552 scenarios from respondents where sensor appropriateness falls below baseline norms. All the sensitive context archetypes that are available in Table 3 share one common finding, that the participants generally do not want their data recorded. Yet sensing and recording data is fundamental for AR to work in the first place. Hence, these sensitive context archetypes could form the basis for enhancing privacy for everyday AR headsets, prompting automated restrictions on sensing capabilities based on real-time contextual cues, respective to the headset functionality. Our approach builds on prior research that relied on changing data access based on specific locations [32,60,66], instead, our work proposes acting on the *underlying reasons* that led to locations being perceived as sensitive.

When looking at baseline sensitive context archetype we show that participants feel data collection from any sensor is only appropriate if the sensor is being used to produce some level of functionality rather than '*always-on*'. Generally similar to previous work [27, 31, 36] participants were worried about their headsets front camera capturing personal information such as financial documents [27,31,36], intimate settings [27] and nudity [36]. Our participants share the same worries, which is reflected in the sensitive context archetypes. More importantly, our results show that participants are worried about more sensors than just the front-camera recording and capturing private moments in their lives. Similar to previous work [27, 31, 32, 36], our results share the front camera being one of the most inappropriate sensors to be active within an sensitive context archetype, but our results go beyond and show the microphone, eye-tracking, and EEG were seen as just as inappropriate. Our participants are also worried about their GPS data being tracked and giving away information. One participant mentioned the risk that GPS data being exposed would have on their healthcare, such as visiting an abortion clinic or life insurance being invalidated. Participants were also more worried about multiple sensors capturing private information than just the front-camera.

5.1 Sensors and What To Do With Them

5.1.1 Headset Usage in an Everyday AR Future

When looking at the archetypes it is important to mention how they would work in the context of what true everyday AR is. One could ask if people will really use their headsets *everywhere*, like bathrooms or at home. Yet despite the various legal and social restrictions, people already use devices with similar sensors in private locations, such as their homes and bathrooms, and also in social locations, such as restaurants and parties. It is common to see smart home assistants and IoT devices being used in the home, or wearing wearable health trackers that collect biometric data throughout the day. Based on previous technology usage, it is not unreasonable to expect people to keep wearing and using, AR glasses in contexts such as these, and perhaps even more so given the headset could be more discreet to use whilst others remain unaware. The creation of sensitive context archetypes would lead both user's and bystanders' data to be more private than if the archetypes did not exist.

5.1.2 Access Control as a First Line of Defence

Both literature [1, 2, 17, 32, 55, 60, 66, 70] and our results suggest that instead of configuring binary permissions once and allowing or denying applications full sensor access, sensors should be limited within everyday AR based on context and need - we would suggest limiting sensors based on sensitive context archetypes. Solutions that *balance functionality and privacy* must be explored to prevent unnecessary curtailment of device functionality - undermining the very reasons by which we use everyday AR. For example, a microphone in a context such as at work was rated the least appropriate to be active. Instead of being continuously active, the sensor could become activated when connected to specific WiFi networks, or via

an interaction, e.g. using a voice assistant to ask a question, which differs significantly from a microphone that is '*always-on*'.

5.1.3 The Problem with Access Control?

However, access to AR sensors is invariably requested for a reason; each sensor access request should match an application's functionality [22]. Thus, proposing a binary access control to deny specific sensors when the user is in a sensitive location is subpar. If we consider manual, user-driven access control, there is an additional burden on the user. Conversely, if we automated access control (e.g. denying access to a sensor when dropping below baseline appropriateness), such a solution would be naive, as the functionality that required the sensing will prevent the application from running correctly in a breadth of contexts, undermining the purpose of all-day wear of such devices. Blocking sensor access entirely from the application is not a reasonable substitution for privacy.

5.1.4 Granular Sensing and Fine-Grained Permissions

Instead, we recommend exploring new flexible methods to maintain functionality using less problematic data. Past work proposed alternative methods such as using Recognisers [29] to enable *fine-grained permissions*. When the user enters a sensitive context archetype, the extent of how fine-grained the permissions are allows developers more freedom to enhance both privacy and user experience. Roesner *et al.*'s [60] world-based access control moved the burden for managing different levels of data access from the developer to the headset. The access control provides the application with the appropriate recognisers that should be ready to run in the location. Another method is to sanitise the raw sensor data, for example, lowering the data fidelity [1, 8, 9, 66] or differential privacy [38, 52, 65] for all sensors our participants stated as "*neither appropriate nor inappropriate*" or below. Hence, if a user was at a beach, the headset should run the "*Outdoor Public Location*" data access level. However, once the headset notices the user is actually at a nudist beach, the headset should change to the "*Modesty and Nudity*" data access level, which has more conservative rules.

Our results show that each of the sensors within all the archetypes is considered inappropriate to be active. The sensitive context archetypes are designed to be broad and cover many common everyday AR uses. When balancing privacy and the applications working, our results show our participants want minimal (if any) data collection within sensitive context archetypes. This may change if validated by implementing the archetypes at face value using current technology. Currently, AR users can only provide full data access or none at all [1]; balancing privacy and functionality should not have to be a dichotomous choice [20], both our work and previous literature [7, 32, 55, 59, 60, 66] point towards different privacy considerations for different locations and contexts.

Future AR headsets should be privacy-preserving by never allowing full access to sensors and using '*Privacy by Design*' principles [34]. Corbett *et al.* [7] introduced '*BystandAR*' which allows on-device processing for the front RGB and depth camera raw data feed to protect the identity of AR bystanders with 98.14% accuracy with the main subject being visible 96.27% of time. Future AR headsets should implement a combination of fine-grained permissions and conditional data filtering. Front-facing UI such as Abraham *et al.*'s [1] user experience-based permission system that gives users different data fidelity options when first opening an application would allow users to set the appropriate permissions for the current context. This could be paired with background processes such as '*BystandAR*' [7] or a '*world based permission system*' [60] with the Sensitive Context Archetypes and sensor configurations provided in Table 3 to account for the changes in privacy considerations during daily AR wear.

5.2 Sensitive Context Archetypes and Defining Them

5.2.1 Further Mapping Existing and Emerging Archetypes

In addition to collecting more data from different demographics and cultures as highlighted in section 3.5 to refine the existing archetypes, future work needs to assess baseline everyday AR sensing attitudes globally. Our approach is promising as whilst there are a near-unlimited number of locations that a device could be in, we suggest that these underlying sensitive context archetypes may be far fewer in number, allowing for more specific privacy policies that reflect the nuances of everyday life. It is imperative to enable AR headsets to adapt and personalise data access for each user dynamically using sensitive context archetypes. For example, consider a workplace at lunchtime - a pure geo-fenced approach [72] might consider the entire location "*confidential*" at all times. In contrast, an archetype-based approach would understand the difference between a shared office and a canteen and adapt to the context's privacy concerns. Hence, subsequently shifting the responsibility of re-configuring data access settings from the user to the headset. Inferring the archetype based on the context may in itself have privacy implications. Nevertheless, for this work, we suggest inferring archetypes should be done locally on the AR headset

5.2.2 Understanding What Archetypes Apply and When

Determining what sensitive context archetypes apply with a high degree of certainty is a practical challenge. Achieving context detection at an adequate level of accuracy could involve another layer between the raw sensor data stream and the application, using pre-trained Machine Learning (ML) models to detect specific characteristics in a given scene. Some of our archetypes are more obviously "detectable" than others, e.g. detecting nudity [18, 33]. However, it is considerably more challenging to train a model to identify if the bystander is about to tell a personal story they would like not to be recorded or to differentiate if the user wants solitude or is just secluded. AR devices with dedicated ML co-processors (such as Google Tensor [21] or the Apple Neural Engine [3]) could run mobile lightweight models in the background, applied to snapshots of e.g. camera, audio, and GPS data to detect applicable archetypes. However, practical concerns arise, such as how a headset can potentially run such models indefinitely and be lightweight, with a battery capacity to last the whole day, and cost-effectiveness is challenging. With the understanding of all the different archetypes, research will need to consider whether there is an effective trade-off here. Is the privacy benefits of such an approach worth the computational cost, or is further work required to build computationally efficient algorithms that detect such archetypes before this approach becomes feasible? Finally, privacy is personal and built on social constructs and law [43, 53, 54, 64]. Thus, it is relevant to consider whether sensitive context archetypes alone would be sufficient, for example, how the varying presence of bystanders, both known and unknown to the user, is to be accounted for in the archetypes.

6 Conclusion

Everyday AR headsets have various sensing capabilities and will be worn throughout the day, even in sensitive contexts where data collection may be undesired by users. Hence, we presented locations and the attributes that create sensitive contexts within those locations. We found that contextual factors within a location impact which sensors should be active compared to a general data access level. Our results present seven sensitive context archetypes collated with a set of actual locations and discuss how to configure data access within those contexts. Our work advocates for dynamic AR data access controls that adjust for the locations and contexts the user encounters daily. Moreover, our results work towards understanding when and why AR users want more privacy to create a more privacy-conscious AR future.

7 Supplemental Materials

All supplemental materials are available within the attached zip file. The contents include (1) the AR onboarding, (2) the full questionnaire used, (3) the final qualitative codebook, including all of the reported locations, and (4) the full pairwise comparisons.

Acknowledgments

This work was funded by UK Research and Innovation (UKRI) under the UK government's Horizon Europe funding guarantee [EP/Z000068/1] (AUGSOC - https://augsoc-project.org/) and an EPSRC DTP studentship (EP/T517896/1).

References

[1] M. Abraham, M. Mcgill, and M. Khamis. What you experience is what we collect: User experience based fine-grained permissions for everyday augmented reality. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pp. 1–24, 2024. 1, 2, 7, 8

[2] M. Abraham, P. Saeghe, M. McGill, and M. Khamis. Implications of xr on privacy, security and behaviour: Insights from experts. In *NordiCHI '22: Proceedings of the 12th Nordic Conference on Human-Computer Interaction: Participative computing for sustainable futures*, 2022. 1, 7

[3] Apple. Deploying transformers on the apple neural engine, June 2022. 8

[4] J. Artuso and K. , Sharma. Combining vr and neurotechnology with openbci's galea, Nov 2022. 3

[5] L. Bajorunaite, S. Brewster, and J. Williamson. Virtual reality in transit: how acceptable is vr use on public transport? In *2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, 2021. 1

[6] W. S. Cleveland and R. McGill. Graphical perception: Theory, experimentation, and application to the development of graphical methods. *Journal of the American statistical association*, 79(387):531–554, 1984. 4

[7] M. Corbett, B. David-John, J. Shang, Y. C. Hu, and B. Ji. Bystandar: Protecting bystander visual data in augmented reality systems. In *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services*, pp. 370–382, 2023. 2, 8

[8] B. David-John, K. Butler, and E. Jain. For your eyes only: Privacy-preserving eye-tracking datasets. In *2022 Symposium on Eye Tracking Research and Applications*, pp. 1–6, 2022. 8

[9] B. David-John, D. Hosfelt, K. Butler, and E. Jain. A privacy-preserving approach to streaming eye-tracking data. *IEEE Transactions on Visualization and Computer Graphics*, 27(5):2555–2565, 2021. 2, 8

[10] T. Denning, Z. Dehlawi, and T. Kohno. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2377–2386, 2014. 2

[11] B. Efron. Missing data, imputation, and the bootstrap. *Journal of the American Statistical Association*, 89(426):463–475, 1994. 4

[12] C. Eghtebas, F. Kiss, M. Koelle, and P. Woźniak. Advantage and misuse of vision augmentation–exploring user perceptions and attitudes using a zoom prototype. In *Augmented Humans Conference 2021*, pp. 77–85, 2021. 1

[13] L. A. Elkin, M. Kay, J. J. Higgins, and J. O. Wobbrock. An aligned rank transform procedure for multifactor contrast tests. In *The 34th annual ACM symposium on user interface software and technology*, pp. 754–768, 2021. 4, 6

[14] L. A. Elkin, M. Kay, J. J. Higgins, and J. O. Wobbrock. Artool- align-and-rank data for nonparametric factorial anova, February 2023. 4

[15] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner. Android permissions demystified. In *Proceedings of the 18th ACM conference on Computer and communications security*, pp. 627–638, 2011. 1

[16] A. P. Field. *Discovering statistics using IBM SPSS statistics*. SAGE Publications, London, 5th ed., 2017. 4

[17] A. Gallardo, C. Choy, J. Juneja, E. Bozkir, C. Cobb, L. Bauer, and L. Cranor. Speculative privacy concerns about ar glasses data collection. *Proceedings on Privacy Enhancing Technologies*, 4:416–435, 2023. 1, 3, 7

[18] D. Ganguly, M. H. Mofrad, and A. Kovashka. Detecting sexually provocative images. In *2017 IEEE winter conference on applications of computer vision (WACV)*, pp. 660–668. IEEE, 2017. 8

[19] N. Gerber, P. Gerber, and M. Volkamer. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security*, 77:226–261, 2018. 3

[20] P. Gerber, M. Volkamer, and K. Renaud. Usability versus privacy instead of usable privacy: Google's balancing act between usability and privacy. *Acm Sigcas Computers and Society*, 45(1):16–21, 2015. 8

[21] Google. How google tensor powers up pixel phones., 2022. 8

[22] Google. Request app permissions, April 2024. 1, 8

[23] J. Gugenheimer, C. Mai, M. McGill, J. Williamson, F. Steinicke, and K. Perlin. Challenges using head-mounted displays in shared and social spaces. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, pp. 1–8, 2019. 1

[24] J. Ha, S. Park, and C.-H. Im. 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*, 16:758537, 2022. 3

[25] S. Hickson, N. Dufour, A. Sud, V. Kwatra, and I. Essa. Eyemotion: Classifying facial expressions in vr using eye-tracking cameras. In *2019 IEEE Winter Conference on Applications of Computer Vision (WACV)*, pp. 1626–1635. IEEE, 2019. 1

[26] M. HoloLense 2. About hololens 2, Mar 2023. 1, 3

[27] R. Hoyle, R. Templeman, D. Anthony, D. Crandall, and A. Kapadia. Sensitive lifelogs: A privacy analysis of photos from wearable cameras. In *Proceedings of the 33rd Annual ACM conference on human factors in computing systems*, pp. 1645–1648, 2015. 2, 7

[28] J. Hu, A. Iosifescu, and R. LiKamWa. Lenscap: split-process framework for fine-grained visual privacy control for augmented reality apps. In *Proceedings of the 19th annual international conference on mobile systems, applications, and services*, pp. 14–27, 2021. 2

[29] S. Jana, D. Molnar, A. Moshchuk, A. Dunn, B. Livshits, H. J. Wang, and E. Ofek. Enabling {Fine-Grained} permissions for augmented reality applications with recognizers. In *22nd USENIX Security Symposium (USENIX Security 13)*, pp. 415–430, 2013. 1, 8

[30] R. Johnstone, N. McDonnell, and J. R. Williamson. When virtuality surpasses reality: possible futures of ubiquitous xr. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, pp. 1–8, 2022. 1

[31] M. Koelle, S. Ananthanarayan, S. Czupalla, W. Heuten, and S. Boll. Your smart glasses' camera bothers me! exploring opt-in and opt-out gestures for privacy mediation. In *Proceedings of the 10th Nordic Conference on Human-Computer Interaction*, pp. 473–481, 2018. 2, 7

[32] M. Koelle, M. Kranz, and A. Möller. 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*, pp. 362–372, 2015. 2, 7, 8

[33] K. Kusrini, A. Setyanto, I. M. A. Agastya, H. Hartatik, K. Chandramouli, and E. Izquierdo. a deep-learning framework for accurate and robust detection of adult content. *Journal of Engineering Science and Technology*, 2022. 8

[34] M. Langheinrich. Privacy by design—principles of privacy-aware ubiquitous systems. In *International conference on ubiquitous computing*, pp. 273–291. Springer, 2001. 8

[35] K. Lebeck, K. Ruth, T. Kohno, and F. Roesner. Towards security and privacy for multi-user augmented reality: Foundations with end users. In *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 392–408. IEEE, 2018. 2

[36] L. Lee, J. Lee, S. Egelman, and D. Wagner. Information disclosure concerns in the age of wearable computing. In *NDSS Workshop on Usable Security (USEC)*, vol. 1, pp. 1–10, 2016. 2, 7

[37] R. J. Little and D. B. Rubin. *Statistical analysis with missing data*, vol. 793. John Wiley & Sons, 2019. 4

[38] A. Liu, L. Xia, A. Duchowski, R. Bailey, K. Holmqvist, and E. Jain.

Differential privacy for eye-tracking data. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications*, pp. 1–10, 2019. 8

[39] F. Liu, G. Xu, Q. Wu, Q. Du, W. Jia, and M. Tan. Cascade reasoning network for text-based visual question answering. In *Proceedings of the 28th ACM International Conference on Multimedia*, pp. 4060–4069, 2020. 1, 2

[40] N. K. Malhotra, S. S. Kim, and J. Agarwal. Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information systems research*, 15(4):336–355, 2004. 3

[41] P. Mallojula, J. Ahmad, F. Li, and B. Luo. You are (not) who your peers are: Identification of potentially excessive permission requests in android apps. In *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 114–121. IEEE, 2021. 1, 2

[42] S. Mansour, P. Knierim, J. O'Hagan, F. Alt, and F. Mathis. Bans: Evaluation of bystander awareness notification systems for productivity in vr. In *Network and Distributed Systems Security (NDSS) Symposium*, 2023. 2

[43] K. Martin. Understanding privacy online: Development of a social contract approach to privacy. *Journal of business ethics*, 137:551–569, 2016. 2, 8

[44] P. Mayring. *Qualitative content analysis: theoretical foundation, basic procedures and software solution*. AUT, 2014. 4

[45] M. McGill, S. Brewster, D. P. De Sa Medeiros, S. Bovet, M. Gutierrez, and A. Kehoe. Creating and augmenting keyboards for extended reality with the k eyboard a ugmentation t oolkit. *ACM Transactions on Computer-Human Interaction*, 29(2):1–39, 2022. 1

[46] M. Mcgill, A. Kehoe, E. Freeman, and S. Brewster. Expanding the bounds of seated virtual workspaces. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 27(3):1–40, 2020. 1

[47] M. McGill, G. Li, A. Ng, L. Bajorunaite, J. Williamson, F. Pollick, and S. Brewster. Augmented, virtual and mixed reality passenger experiences. In *User Experience Design in the Era of Automated Driving*, pp. 445–475. Springer, 2022. 1

[48] Meta. Meta quest apps must target android 12l starting june 30, Mar 2023. 1

[49] Meta. Meta quest tech specs, Sep 2023. 3

[50] A. H. Mhaidli and F. Schaub. Identifying manipulative advertising techniques in xr through scenario construction. In *Proceedings of the 2021 chi conference on human factors in computing systems*, pp. 1–18, 2021. 1

[51] P. E. Morris and C. O. Fritz. Effect sizes in memory research. *Memory*, 21(7):832–842, 2013. 4

[52] V. C. Nair, G. Munilla-Garrido, and D. Song. Going incognito in the metaverse: Achieving theoretically optimal privacy-usability tradeoffs in vr. In *Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology*, pp. 1–16, 2023. 8

[53] H. Nissenbaum. Privacy as contextual integrity. *Wash. L. Rev.*, 79:119, 2004. 2, 8

[54] H. Nissenbaum. A contextual approach to privacy online. *Daedalus*, 140(4):32–48, 2011. 2, 8

[55] J. O'Hagan, P. Saeghe, J. Gugenheimer, D. Medeiros, K. Marky, M. Khamis, and M. McGill. 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):1–35, 2023. 1, 2, 7, 8

[56] A. Panicker, N. Nurain, Z. Ibrahim, C.-H. Wang, S. W. Ha, Y. Wu, K. Connelly, K. A. Siek, and C.-F. Chung. Understanding fraudulence in online qualitative studies: From the researcher's perspective. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pp. 1–17, 2024. 3

[57] Qualtrics. Fraud detection, July 2024. 3

[58] Qualtrics. Qualtrics, July 2024. 3

[59] F. Roesner, T. Kohno, and D. Molnar. Security and privacy for augmented reality systems. *Communications of the ACM*, 57(4):88–96, 2014. 1, 8

[60] F. Roesner, D. Molnar, A. Moshchuk, T. Kohno, and H. J. Wang. World-driven access control for continuous sensing. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, pp. 1169–1181, 2014. 1, 2, 7, 8

[61] A. Schmidt, M. Beigl, and H.-W. Gellersen. There is more to context than location. *Computers & Graphics*, 23(6):893–901, 1999. 2

[62] S. Schneegass, R. Poguntke, and T. Machulla. Understanding the impact of information representation on willingness to share information. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pp. 1–6, 2019. 4

[63] G. L. Scoccia, A. Peruma, V. Pujols, I. Malavolta, and D. E. Krutz. Permission issues in open-source android apps: An exploratory study. In *2019 19th International Working Conference on Source Code Analysis and Manipulation (SCAM)*, pp. 238–249. IEEE, 2019. 1, 2

[64] H. Smith, T. Dinev, and H. Xu. Information privacy research: an interdisciplinary review. mis q. 35 (4): 989–1015, 2011. 8

[65] J. Steil, I. Hagestedt, M. X. Huang, and A. Bulling. Privacy-aware eye tracking using differential privacy. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications*, pp. 1–9, 2019. 8

[66] J. Steil, M. Koelle, W. Heuten, S. Boll, and A. Bulling. Privaceye: privacy-preserving head-mounted eye tracking using egocentric scene image and eye movement features. In *Proceedings of the 11th ACM symposium on eye tracking research & applications*, pp. 1–10, 2019. 2, 3, 7, 8

[67] M. Tahaei, R. Abu-Salma, and A. Rashid. Stuck in the permissions with you: Developer & end-user perspectives on app permissions & their privacy ramifications. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23. Association for Computing Machinery, New York, NY, USA, 2023. doi: 10.1145/3544548.3581060 1, 2

[68] R.-D. Vatavu, P. Saeghe, T. Chambel, V. Vinayagamoorthy, and M. F. Ursu. Conceptualizing augmented reality television for the living room. In *ACM International Conference on interactive media experiences*, pp. 1–12, 2020. 1

[69] J. O. Wobbrock, L. Findlater, D. Gergle, and J. J. Higgins. The aligned rank transform for nonparametric factorial analyses using only anova procedures. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pp. 143–146, 2011. 4

[70] K. Wolf, K. Marky, and M. Funk. We should start thinking about privacy implications of sonic input in everyday augmented reality! *Mensch und Computer*, 2018. 2, 7

[71] K. Wolf, A. Schmidt, A. Bexheti, and M. Langheinrich. Lifelogging: You're wearing a camera? *IEEE Pervasive Computing*, 13(03):8–12, 2014. 1, 2

[72] T. Young. What is geofencing? everything you need to know about location-based marketing, December 2022. 8