Towards Security and Privacy for Multi-User Augmented Reality: Foundations with End Users

Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, Franziska Roesner
Paul G. Allen School of Computer Science & Engineering
University of Washington
{kklebeck, kcr32, yoshi, franzi}@cs.washington.edu
https://ar-sec.cs.washington.edu

***Abstract*—Immersive augmented reality (AR) technologies are becoming a reality. Prior works have identified security and privacy risks raised by these technologies, primarily considering individual users or AR devices. However, we make two key observations: (1) users will not always use AR in isolation, but also in ecosystems of other users, and (2) since immersive AR devices have only recently become available, the risks of AR have been largely hypothetical to date. To provide a foundation for understanding and addressing the security and privacy challenges of emerging AR technologies, grounded in the experiences of real users, we conduct a qualitative lab study with an immersive AR headset, the Microsoft HoloLens. We conduct our study in pairs — 22 participants across 11 pairs — wherein participants engage in paired and individual (but physically co-located) HoloLens activities. Through semi-structured interviews, we explore participants' security, privacy, and other concerns, raising key findings. For example, we find that despite the HoloLens's limitations, participants were easily immersed, treating virtual objects as real (e.g., stepping around them for fear of tripping). We also uncover numerous security, privacy, and safety concerns unique to AR (e.g., deceptive virtual objects misleading users about the real world), and a need for access control among users to manage shared physical spaces and virtual content embedded in those spaces. Our findings give us the opportunity to identify broader lessons and key challenges to inform the design of emerging single- and multi-user AR technologies.**

I. Introduction

Augmented reality (AR) technologies, which overlay virtual content on users' perceptions of the physical world, are now a commercial reality. Recent years saw the success of the smartphone AR app Pokémon Go [44], and more immersive AR technologies such as head-mounted displays [22, 30] and automotive AR windshields [5] are shipping or on the horizon.

Within the computer security and privacy community, prior efforts have made significant progress toward anticipating and addressing security, privacy, and safety challenges raised by AR technologies [12, 37]. For example, these works have sought to defend against buggy or malicious apps on a user's device that may record privacy-sensitive information from the user's surroundings [16, 23, 36, 45, 48] or disrupt the user's view of the world (e.g., by occluding oncoming vehicles or pedestrians in the road) [25, 26], as well as the risks that a user's AR device might pose to bystanders [15, 38].

While valuable for the problems that they do tackle, we observe two critical gaps in prior works. First, they consider primarily *individual* AR users and their devices. However, emerging AR technologies will not be used only by individual users in isolation, but also by multiple users, each with their own AR device — including users who share the same physical space and may interact with shared virtual content embedded in this space. Indeed, existing AR research efforts (e.g., [24, 43, 49]), as well as already deployed AR apps such as Pokémon Go, rely on interactions between multiple, often physically co-located, users. We refer to AR systems that support these interactions as *multi-user AR systems*, and we argue that considering the risks that might arise for users of such systems is critical to the success of future AR technologies. Precursors of such risks have already begun to appear in the wild today, e.g., recent "vandalism" of augmented reality art in Snapchat [27].

Second, we observe that immersive AR technologies such as Microsoft's HoloLens [22] have only recently become available. Thus, even in the context of individual users or AR devices, prior works have focused on *conjectured* security, privacy, and safety concerns that arise in anticipation of emerging AR technologies, but that are not necessarily grounded in users' experiences with the technologies themselves.

Our Goals and Approach. We aim to bridge the above gaps by investigating the concerns of end users grounded in their experiences with real AR technologies, in both single- *and* multi-user contexts. That is, we strive to uncover a broad spectrum of risks that AR users may face — which may stem from buggy or malicious apps *or* other misbehaving users — and to identify challenges that must be addressed to support rich single- and multi-user experiences. Since immersive AR systems are only just emerging, we cannot fully predict users' expectations of or interactions with these technologies, nor their interpersonal interactions while using them. Thus, we directly study end users engaging with real AR technology, and with each other, through an in-lab partner study using the Microsoft HoloLens, an immersive AR headset (see Figure 1). Ultimately, we strive to provide a broad foundation for understanding and addressing the computer security and privacy challenges that emerging AR technologies will present.

Research Questions. In support of our above goals, we design our study to investigate the following research questions:

1) *RQ1:* What expectations and behaviors arise for users engaging with a real, immersive AR technology, and what interpersonal interactions arise *between* these users?
2) *RQ2:* What concerns arise for users in practice — involving both single- and multi-user experiences — given the opportunity to interact with other users and applications on an immersive AR device?

Finally, since prior work has considered technical challenges with security primarily for single-user AR systems, we ask:

3) *RQ3:* What new system design challenges and opportunities arise for security and privacy in *multi-user* AR?

Methodology and Findings Highlights. We conducted an in-lab, qualitative user study with the HoloLens. We recruited pairs of participants (22 individuals in 11 pairs), combining hands-on HoloLens activities with semi-structured interview questions. Following accepted methods for qualitative research [10, 19, 20], we focused in depth on a small number of participants until we reached saturation of themes.

Among other findings detailed in Section IV, we find (to our surprise) that the HoloLens, despite its technical limitations, provided an immersive experience that shaped participants' expectations of and interactions with virtual content (Section IV-A). Notably, participants often assumed that virtual objects behave like physical objects — for instance, instinctively stepping around virtual objects or assuming (sometimes incorrectly) that both they and their physically co-located partner could see the same virtual objects. As we discuss, such expectations can be leveraged adversarially. Further, participants' interpersonal interactions (Section IV-B) — though lighthearted in the context of the study — hinted at potential conflicts and challenges. For example, some participants placed virtual objects in each others' faces or attempted to steal control of objects from each other.

Once participants had the opportunity to experience immersive AR technology firsthand, we asked them to consider specific adversarial scenarios, involving both other users and untrusted applications. In response, participants raised a rich variety of concerns about risks that might arise from these scenarios in both single- and multi-user contexts (Section IV-C). These concerns both corroborate and enrich those considered in prior work (e.g., the risk of deceiving someone about the physical world) and raise new issues around interpersonal interactions (e.g., concerns about other AR users destroying or manipulating one's virtual objects).

Finally, whereas prior technical work focused on securing single-user AR experiences, our results raise new design challenges for securely supporting multi-user AR interactions. For example, participants' interactions highlighted tensions around ownership and access control of virtual objects (Section IV-D).

Contributions. In summary, we contribute the following:

1) *Problem Identification:* We identify the fundamental need — largely unaddressed in prior work — to consider security, privacy, and safety for emerging single- *and* multi-user AR technologies, grounded in the experiences and interactions of end users.
2) *Study of End Users with Real AR Technology:* Through a user study with pairs of participants using the HoloLens, we identify and investigate critical research questions in support of the above goal.
3) *Foundation for Secure AR Systems:* Our work provides a foundation for addressing the security, privacy, and safety risks that will imminently arise for both single- and multi-user AR scenarios, and we raise key research and design challenges to inform future defensive directions.

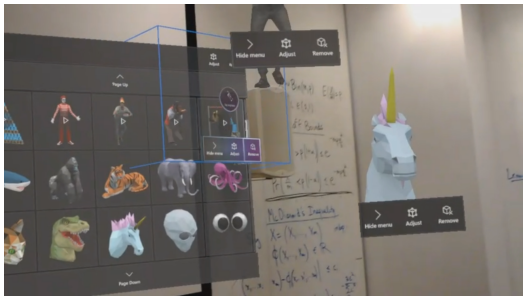


Fig. 1: A first-person view of virtual objects, or "holograms", as seen through the HoloLens head mounted display, including 2D menus and 3D objects.

II. Background and Motivation

We begin with background on augmented reality and prior work on AR security and privacy to motivate our work.

Augmented Reality. AR technologies have recently entered consumer markets, with smartphones putting basic AR capabilities in the hands of millions of users. Popular apps such as Pokémon Go showcased the success of smartphone-based AR [44], and development frameworks such as Apple's ARKit [2], Google's Tango [3], and Facebook's AR Studio [1] are enabling new AR experiences on phones. However, the vision of AR extends beyond smartphones, aiming to convincingly blend virtual content with a user's perception of the physical world. Immersive AR technologies that move towards this vision are emerging, such as Microsoft's HoloLens [22] and Meta's Meta2 glasses [30]. Other examples abound, e.g., in the automotive industry [5] and military [32], with the AR market expected to grow substantially in coming years [29].

Significant research and commercial efforts have explored the use of AR for both single- and multi-user applications. Single-user examples include real-time text translation [4], visual informational overlays about users' geographic surroundings (e.g., nearby hotels, restaurants, or landmarks) [50], and many more. In contrast, other compelling AR use cases are fundamentally multi-user. For example, Pokémon Go is a multi-user game in which physically co-located players can virtually battle each other for control of "Pokémon gyms" associated with real-world landmarks, and HoloLens has partnered with Autodesk to enable collaborative 3D product design [52]. Moreover, prior research efforts have also explored positive opportunities for engagement between multiple AR users in-

cluding tabletop multiplayer games, workplace collaboration, and mathematical educational tools [24, 43, 49].

Security and Privacy for AR. While emerging AR technologies show great potential, the computer security and privacy community has begun to identify and address serious security, privacy, and safety risks that they present [12, 13, 37]. Many of these efforts focus on the risks that individual AR users might face from malicious or buggy apps on their own devices. For example, some address input privacy — preventing the leakage of sensitive sensor data (e.g., images of faces or sensitive documents) to untrusted apps [16, 23, 36, 45, 48]. Others consider output security — preventing apps from displaying unwanted or harmful content (e.g., virtual objects that startle the user or obstruct their view of the physical world) [25, 26]. Prior works have also sought to understand and mitigate the privacy risks that bystanders may face due to non-consensual recording by the devices of nearby AR users [15, 38].

A limited body of work has also begun investigating security and privacy protections for multi-user interactions. For example, some have proposed abstractions for virtual object privacy in shared AR settings [8, 9], while others have proposed mechanisms for securely pairing multiple AR devices for cross-device communication [18, 40].

These works and others provide a valuable foundation, but we observe two important gaps. First, prior work almost exclusively considers *individual* AR users in isolation or bystanders. However, as illustrated by the above examples, AR technologies may also be used by *multiple* users interacting with shared virtual content and/or in the same physical space. Thus, the risks that users will face may stem not only from buggy or malicious apps, but also from other users, and these risks have not yet been studied or addressed. Second, while prior work has studied general experiences and expectations of end users of AR (e.g., [33–35]), prior work on security and privacy for AR has not directly studied end users — due in part to the fact that real, immersive AR technologies have only recently become available.

Further afield from AR, digital interactions between physically co-located users have been studied in the context of interactive tabletop interfaces, including the challenges of governing personal territory [39] and preventing conflicts between users [31]. We identify related challenges for multi-user AR that may be informed by these works. Researchers have also studied the applicability of social norms in virtual reality, e.g., [46, 51]. As AR technologies become more sophisticated and more widely deployed, the study of maintaining (or changing) social norms in AR environments — which blend both virtual and real content — will also become valuable.

Goals and Focus of This Work. The above gaps in prior work together motivate our goals and supporting research questions laid out in Section I. By exploring the expectations and behaviors of real users (RQ1), as well as their concerns involving both single- and multi-user AR experiences (RQ2), we seek to provide a foundation for understanding and addressing the computer security and privacy challenges of emerging AR technologies — including new challenges that arise from multi-user systems in particular (RQ3). In studying multi-user AR, we focus primarily on physically co-located users, rather than remote AR interactions like telepresence. Though we return to a discussion of remote interactions in Section V, we observe that physically co-located interactions exercise a fundamentally unique property of AR, compared to traditional digital interactions: the ability to support simultaneous views of shared physical *and* virtual worlds.

III. Methodology

A. Methodology Overview

We designed a user study to investigate our research questions described in Section I, in support of our above goals. Before presenting the full details of our methodology, we highlight several key decisions we made in designing our study.

Qualitative, In-Lab Partner Study. Since this research space remains largely unexplored, we designed an *exploratory, qualitative* study. Compared to a quantitative methodology, a qualitative study allowed us to explore a broad spectrum of expectations, interactions, and concerns, with limited need for preconceived notions of what we might find. Furthermore, immersive AR devices are not yet widely deployed amongst consumers, so we conducted our study *in-lab*. We brought in participants to use the Microsoft HoloLens, one of the most sophisticated, immersive AR devices commercially available today; we provide further details on it in Section III-C.

Given our goal of studying multi-user AR systems, we conducted our study with *pairs of participants*. In an effort to ensure that participants felt comfortable enough with each other to explore, converse, and potentially push boundaries while interacting during the study, we recruited pairs with pre-existing relationships. Additionally, because we hoped to observe participants' natural expectations and behaviors before they were shaped by the actual affordances of the HoloLens, we sought participants with *no prior HoloLens experience*.

Two Study Phases: HoloLens Activities and Interviews. We divided our study into two main phases: an activity phase in which we observed participants interacting with several HoloLens apps, and a semi-structured interview phase.

The activity-based phase allowed us to observe participants in real time as they interacted with applications and each other, thereby organically surfacing their expectations, reactions, and potential conflicts. We carefully selected HoloLens apps (and in one case, created one ourselves) that would provide participants with both single- and multi-user AR experiences — we detail the specific apps we used in Section III-D below.

By providing participants with hands-on HoloLens experiences, we sought to enable them to think more concretely about their potential concerns of immersive AR technologies in both single- and multi-user contexts. We designed the second, interview-based phase of the study to surface these concerns. Though we found that our partner study design naturally encouraged participants to think adversarially, we did not prime them to consider any specific threats. Rather, we asked open-ended questions about their potential concerns in AR scenarios involving different stakeholders (including other AR users, apps installed on their devices, and bystanders).

B. Recruitment, Screening, and Ethics

We recruited participants by advertising our study on mailing lists, on a local neighborhood Facebook group, and by asking personal contacts to forward our study information to additional mailing lists. Candidates completed our screening survey indicating any AR devices they had used, demographics (age, gender, profession) and contact information (name, email address), and their relationship with their potential partner (e.g., friends, co-workers, spouses). We selected pairs who reported no prior experience using the HoloLens or similar AR devices. Participants who completed the interview were each compensated with a $15 Amazon gift card.

This study was approved by our University's IRB. We did not ask participants to reveal sensitive information, or to perform dangerous tasks while using a HoloLens. Each participant provided informed consent to participate in the study and to be audio/video recorded. We stored all recordings on password-protected drives, removing any personally identifying information from notes and transcripts. We also informed participants that the HoloLens may cause discomfort (such as eye strain or nausea) for certain individuals, and that they could stop the study at any time if they felt discomfort. We also informed participants of Microsoft's own health and safety information for the HoloLens, providing it upon request.

C. Setup and Hardware

We describe below our study setup and hardware, beginning with details about the Microsoft HoloLens.

HoloLens Details. The HoloLens [22] is an untethered head-mounted display available in a "Developer Edition" for $3,000. Users see virtual objects, or *holograms*, overlaid on a semi-transparent display through which they can also see the physical world, though the field of view within which holograms appear is small (˜30°x17.5°). The HoloLens has multiple sensors [21] that enable *spatial mapping* — the ability to interpret the geometry of a user's environment and overlay holograms in 3D. For example, a user can place a hologram on a table and view it from different angles as if it were physically present. The HoloLens supports third-party applications installed from an app store and can run a single 3D app at a time. User input is given via a tap gesture with the index finger, voice commands, or a single-button clicker.

Study Setup. We conducted the study in a large conference room of our University building. Participants used HoloLens apps (described below), as well as a Microsoft Surface Pro 3. We used two Windows 10 laptops and HoloLens's "Mixed Reality Capture" functionality to record point-of-view footage. This footage includes a first-person view of the real world, the holograms a user sees, and audio from both the real world and any active application. We also recorded participants from a third-person perspective using a Canon HD camcorder.

D. Study Procedure

Below, we detail the HoloLens apps and interview questions that comprised our study. We developed our procedure in an effort to avoid participant response bias. For the activities, we acted as observers, only engaging with participants if they explicitly asked us questions. We also emphasized that we were not evaluating the apps themselves, to promote more honest opinions. For the interviews, our questions were broad in scope, allowing participants to focus on the themes that stood out to them the most. We did not press participants for responses on topics where they did not have strong opinions.

At a high level, each study involved an activity-based phase and a semi-structured interview. We conducted two pilot studies (with two pairs) and modified our interview questions in response to the pilot results and feedback, to reduce ambiguity and better meet our research goals. (Our results do not include data from the pilots.) We describe our study procedure below, providing additional details (including our concrete semi-structured interview questions) in the appendix.

1) Interview: Prior AR Exposure. As a baseline, we asked participants to discuss prior AR exposure, including devices or apps that they had used or observed others using, as well as depictions of AR in literature or film that they had seen.

2) Activity: Introduction to the HoloLens. Participants next used a HoloLens tutorial app (Figure 2a) to learn gestures and voice commands. They then spent a few minutes exploring the "shell", a single-user app similar to a desktop, from which other apps can be launched and which allows holograms to be placed, mapped to a physical space (Figure 2b). For each participant in a pair, we pre-populated the room with one of two sets of holograms that had some overlap (identical objects placed in the same location), and some differences, to let us observe participants' initial expectations of shared content.

3) Interview: Initial Experience and Brainstorming. After this brief HoloLens exposure, we asked participants to describe their initial impressions of the HoloLens. We then asked them to spend a few minutes brainstorming potential use cases for AR. Though a goal of our study was not to identify concrete use cases, we found through our pilot studies that having participants brainstorm helped them think about AR more concretely and led to more grounded discussions later.

4) Activity: HoloLens Applications. We next asked participants to use each of three apps for five to ten minutes apiece: RoboRaid (Figure 2c, a single-player first-person shooter game), Shared Blocks (Figure 2d, a multi-player app we built that allows users to create and move blocks in a shared space), and Skype for HoloLens. We chose these apps, in addition to the shell, because they cover different aspects of an AR experience that AR users might encounter. Specifically:

- The shell is a single-user app that allows users to freely interact with multiple 3D holograms.
- RoboRaid is a single-user game that is more immersive and active than the shell. However, its procedural gameplay provides less freedom to experiment than the shell.
- Shared Blocks[1] is a multi-user app that we created to

[1]Due to technical difficulties, one pair (P1) instead used Tower Blocks, a shared Jenga-like app available on the HoloLens app store, which is similar to but provides less flexibility than Shared Blocks (e.g., enforcing turns).

allow multiple HoloLens users to interact in a shared virtual space. Users can create blocks that obey physical properties (e.g., gravity), and either user can move or change the color of any existing blocks. To avoid biasing participants [14], we did not reveal that we built this app.
- Skype[2] is a multi-user app involving one HoloLens user and one tablet user. The HoloLens user can draw lines in their view, and can see a window with the tablet user's video; the tablet user sees the HoloLens user's first-person view (including their drawings) and can also draw on the HoloLens user's view of the world. Though Skype involves only one user with a HoloLens, given the lack of available multi-user apps at the time of our study, we included Skype for its free-form interaction capabilities.

We uniformly randomized the order in which each pair used the above apps, in an effort to surface as many ideas from participants as possible; a fixed app ordering would have risked missing themes that might arise from alternate orderings.

5) Interview: Reactions, Concerns, and Multi-User Experiences. Upon the conclusion of all HoloLens activities, we interviewed participants, focusing on the following themes.

General Experience. We began by asking participants to describe their general experience, as well what aspects they found enjoyable, frustrating, confusing, or surprising.

Security, Privacy, Safety, and Other Concerns. We next gave participants the opportunity to raise concerns about AR. Specifically, we asked them to discuss three concrete scenarios, to avoid asking them to think abstractly about AR:

- *Abuse of AR Technology* — how they might harass or disrupt another AR user, or what they might worry about another AR user doing to them.
- *Untrusted Applications* — any concerns they had surrounding applications downloaded from the Internet.
- *Bystanders* — any concerns they would have while acting as a bystander to an AR user that is either a stranger or friend, in either a private or public space.

We emphasize again that while we prompted participants to think about the above concrete scenarios, we designed our questions explicitly to avoid priming participants with *specific* concerns — that is, we did not mention any specific concerns ourselves.

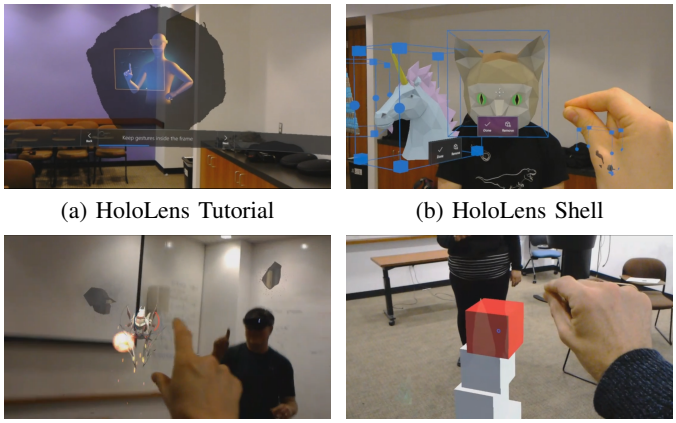
Multi-User Experience. Finally, we asked participants to reflect on their experiences engaging with single- and multi-user apps. We asked if they preferred one setting over the other, and where they might imagine each being useful.

E. Data Analysis

To analyze data from the study, we used a qualitative, inductive (or "bottom-up") process in which we iteratively developed a set of themes, or codes, from the interview transcripts. First, all researchers independently read a subset of the transcripts and developed an initial set of codes; we then met in person to consolidate these codes into a common codebook. Two researchers then independently coded each interview according to that codebook, iteratively modifying the codebook and recoding previously coded interviews as necessary. Because our goal is to surface a breadth of themes that may arise for emerging AR technologies, we chose to identify the presence of each code in each interview, not distinguishing which of the two participants raised the theme. As a result, a single interview could be coded with two conflicting codes (e.g., if each participant assumes their shell environments are shared for different reasons — see Table II).

One primary coder coded all interviews, and two other coders independently coded about half of the interviews each. Our final codebook contains 108 codes. After coding all interviews, we met in person to resolve disagreements where possible, resulting in an average inter-coder agreement of 0.98, measured by Cohen's kappa [11]. Fleiss rates agreement over 0.75 as excellent and 0.40 to 0.75 as intermediate to good agreement [17]. Throughout this paper, we report raw numbers based on the primary coder's values in the cases where disagreements remained due to ambiguity in the interviews.

[2]Two pairs were not able to use Skype (P1, for whom Skype failed completely) and P7 (for whom the drawing feature on the tablet failed).



(a) HoloLens Tutorial (b) HoloLens Shell

(c) RoboRaid (d) Shared Blocks

Fig. 2: First-person views of four of our HoloLens activities (Skype is omitted because it does not work simultaneously with screen capture).

IV. Results

We now turn to our results. As a foundation for uncovering the security and privacy risks of emerging AR systems grounded in the experiences of real users, we begin with a discussion of our participants' concrete expectations and interactions (RQ1) in Sections IV-A and IV-B. We then explore their concerns around multiple actors (RQ2) in Section IV-C, focusing on novel challenges for multi-user AR systems that emerge from these concerns (RQ3) in Section IV-D. While we focus on security- and privacy-related themes in this paper, we initially coded a broader set of additional themes to capture as many of our participants' reactions as possible. However, we found some of those themes less relevant to understanding the security and privacy risks of emerging AR systems, and thus we do not report on those codes. Furthermore, all numbers and major themes reported are directly drawn from our codes, or from direct participant quotes where appropriate. From

ID	Gender	Age	Profession	Partner Relationship	Previous AR Experience
P1-A	Male	25-34	Entrepreneur	Friends / Coworkers	None
P1-B	Male	35-44	Business Owner and Consultant		Other (Unspecified)
P2-A	Female	25-34	Grant Manager	Coworkers	Smartphone-based AR
P2-B	Female	45-54	Fiscal Specialist		None
P3-A	Male	25-34	Software Engineer	Spouses / Significant Others	None
P3-B	Female	25-34	Attorney		None
P4-A	Male	18-24	Undergraduate Student	Friends	None
P4-B	Male	18-24	Undergraduate Student		None
P5-A	Male	25-34	Graduate Student	Friends	None
P5-B	Male	18-24	Graduate Student		Smartphone-based AR
P6-A	Female	35-44	Middle School Teacher	Coworkers	None
P6-B	Male	35-44	Middle School Teacher		Smartphone-based AR*
P7-A	Male	45-54	Author	Spouses / Significant Others	Smartphone-based AR
P7-B	Female	45-54	Attorney		None
P8-A	Female	18-24	Undergraduate Student	Spouses / Significant Others	Smartphone-based AR
P8-B	Male	18-24	Undergraduate Student		Smartphone-based AR
P9-A	Male	25-34	Commissioned Officer, U.S. Air Force	Coworkers	Google Glass
P9-B	Male	35-44	Non-Commissioned Officer, U.S. Air Force		None
P10-A	Male	18-24	Undergraduate Student	Spouses / Significant Others	Smartphone-based AR
P10-B	Male	18-24	Undergraduate Student		Smartphone-based AR
P11-A	Male	25-34	Law Student	Friends	None*
P11-B	Female	25-34	Law Student		Smartphone-based AR

TABLE I: Participant Summary: Our 22 participants (11 pairs), including their demographic information, relationships, and prior AR use. Participants with asterisks (*) revealed during the interview (but not in the pre-screening survey) that they had 3-5 minutes of prior HoloLens experience, but we did not observe qualitative differences in those participants during the study. Participants with identifiers ending in "A" were the HoloLens users during Skype (while "B" used the tablet).

the themes drawn from our data, we derive more reflective discussions surrounding the potential implications that our participants' expectations, behaviors, and concerns may have for the security and privacy of emerging AR systems, beyond the sentiments directly expressed by our participants themselves.

Participants. 34 individuals completed our screening questionnaire, from which we selected 22 (comprising 11 pairs) to interview. We selected participants who reported not having used the HoloLens or a similar device and who were available at times when we conducted the study; we also attempted to maximize diversity among participants. Our participants are summarized in Table I. We conducted interviews during April and May 2017, which lasted approximately 90 minutes each.

A. Expectations of Augmented Reality

Recall that we designed our study to first give participants experience with a few single- and multi-user HoloLens apps, before conducting a semi-structured interview to investigate their potential security and privacy concerns more directly. In this and the following section, we describe our observations from this initial phase of the study in support of our first research question (RQ1) — in this section, focusing on the *expectations* of AR revealed by our participants' interactions with the HoloLens, its apps, and each other.

In presenting these expectations, we also hypothesize ways adversaries (whether other users or malicious or buggy apps) might violate or exploit these expectations. Indeed, in Section IV-C, we will find that many of these concerns arose for our participants themselves after their own hands-on experiences — not just hypothetically for us, as researchers.

High-Level Expectation: AR as Physical. A common theme that seemed to underly a number of our participants' assumptions and behaviors was the treatment of AR content as *an extension of the physical world*, rather than isolated digital content. Indeed, nine pairs mentioned or exhibited the sense that holograms felt "real" or integrated into the real world (e.g., stepping around virtual objects as though they were really present in physical space).

> *"I'm kind of getting mixed up between the AR and the real life."* (P4-A)

The melding of digital and physical worlds is a core part of the vision for AR, and a key aspect that distinguishes AR from other technologies in terms of its positive and possible negative potential. However, the HoloLens as an instantiation of AR still has important limitations, noted sometimes by participants, such as frustrating user input controls (eleven pairs), a bulky form factor (two pairs), and a small field of view (eight pairs). We were thus surprised at the degree to which our participants were immersed *despite* these limitations — that is, the degree to which participants projected physical assumptions onto virtual objects (also referred to as "holograms").

Concretely, the classes of assumptions and behaviors that we observed our participants making included the following:

Assumption: Virtual Objects are Shared. By conducting a partner study, we were able to observe not only participants' expectations of AR in isolation but also in conjunction with other AR users. Recall that participants first used the shell, a single-user app. Most notably, we found that participants often (nine pairs) initially assumed that *both* they and their partner

could see the same holograms, for multiple reasons (Table II). The most common explanation (six pairs) was that the *physical* world is shared. In other words, because both participants see the same physical world, they often expected the *virtual objects* integrated into that world to also be shared.

> *"I kept having the same feeling of . . . 'oh come check this out' and then I was like 'oh yeah I only get to see this'. Because it's like through my eyes and I'm used to being a human, and someone else can literally stand next to me and see what I see."* (P6-B)

AR apps may exhibit different sharing behaviors, with some virtual content private and some public, and violations of a user's expectations about what is shared may expose the user to harm. For example, a user may interact with sensitive virtual content without realizing that other users can see it, or they may inadvertently (e.g., verbally) reveal private information that has been shared with them but not with others who are nearby. These risks raise unique challenges for multi-user AR systems, discussed further in Section IV-D and Section V-A.

Assumption: Virtual Objects Act Like Physical Objects. Our study also surfaced a number of assumptions and behaviors that arise even in single-user AR settings. One such assumption is that virtual objects have similar physical properties as physical objects — for instance, that they will follow basic rules of physics (e.g., not fall through the floor) and that they continue to exist even while not seen, (i.e., object permanence). Indeed, two pairs exhibited a sense of permanence for virtual objects, discussing or treating them as if they were physically present even when the participants could not see them. For example, several minutes after removing the HoloLens, one participant described his experience with a virtual sloth.

> *"I keep trying [to reach out] as if it's still right there. . . . For me, the giant sloth is still filling that half of the room."* (P1-B)

While this sense of immersion enables exciting possibilities, it also raises potential risks. For example, the assumption that virtual objects behave like physical objects could be exploited by adversaries who intentionally violate the expectations of the victim — e.g., to have an object suddenly appear in or disappear from a victim's path, or move in unexpected ways. In fact, many of the concerns voiced directly by participants (Section IV-C) stemmed from this sense of immersion.

Assumption: The Real World Would Still Be Visible. We found that five pairs observed (sometimes with surprise) the HoloLens's ability to display nearly opaque holograms that can occlude a user's view — perhaps contributing to the fact that participants treated virtual objects like physical objects.

> *"And now I feel like the [physical] table is invisible. I feel like I can't see the other side of the table [that is occluded by a virtual block]. That's crazy."* (P9-A)

As AR technologies advance, it will become even harder to identify certain properties of the real world when hidden by virtual objects, a fact that can be exploited adversarially. For example, an adversary could mislead a victim about the nature or even presence of an object in the physical world — e.g., occluding a dangerous physical object, such as a gun, with a benign virtual object. Indeed, this concern was echoed in different forms by our participants (Section IV-C).

Assumptions of Shared Content (Shell Activity)	Number (of 11 pairs)
Assumed content was shared before or during shell	9
Assumption based on video games	1
Assumption based on partner study context	2
Assumption based on the physical world metaphor	6

TABLE II: Shell Expectations: Participant expectations about whether the world would be shared in the shell activity, and why.

Behavior: Avoiding Virtual Obstacles. Assuming that virtual objects act like physical objects also caused participants to adapt their own behaviors. For example, one participant attempted to physically avoid holograms, as they might with physical obstacles on the floor, for fear of tripping.

> *"I'm like worried I'm going to trip on the blocks."* (P4-A)

That is, participants not only *assumed* that virtual objects acted a certain way, but this assumption also affected their own actions and reactions in the physical world. We observe that adversaries can take advantage of this effect, such as by placing holograms to cause a victim to perform physical actions that they might not otherwise perform (e.g., swerving quickly or jumping to avoid a perceived obstacle).

Behavior: Physically Manipulating Virtual Objects. Though the HoloLens supports only a simple "air tap" gesture, ten pairs nevertheless tried, or expressed a desire for, more physically-inspired gestures such as kicking, throwing, or grabbing; and indeed, other emerging AR platforms, such as the Meta 2 [30], support more natural gestures like grabbing virtual objects. Such gestures are desirable from a usability perspective but can also raise risks, including safety risks if an app causes a user to act in a way that is unsafe in their physical environment (e.g., causing them to lose balance), as well as privacy risks if other users or their devices can infer a victim's private interactions with a virtual object through their gestures (as an extension of the classic shoulder-surfing attack, but now from any angle).

B. Inter-Personal Interactions

Our partner study allowed us to observe not only individual participants' expectations and behaviors, but also their interactions with another, physically co-located AR user, continuing our investigation of RQ1 from Section IV-A. Though in the study's context these interactions were lighthearted, they nevertheless surface potential tensions between users that have not been deeply studied in prior work on security and privacy for AR. These interactions also directly informed participants' own concerns, as we discuss in Section IV-C.

Table III details ways in which participants interacted with each other during different activities in the study. We report on these interactions below, and going beyond our observations of participants' behaviors, we raise possible tensions or threats that may arise from them.

Visually Modifying Each Other. We observed that participants often attempted to modify the appearance of their

Multi-User Interaction	Number (of 11 pairs)
Shell: Put holograms on or in front of another person	6
Shared Blocks: Fought over control of a block	3
Shared Blocks: Put blocks on or in front of another person	5
Shared Blocks: Collaboratively built a structure	5
RoboRaid: Shot at another person	6
Skype: Drew on another person	7

TABLE III: Example Interactions: What pairs of participants did to or with each other during different activities. (Note that the Shared Blocks numbers are out of 10, and the Skype number is out of 9, because those apps failed during some studies.)

partner (or the researchers) using virtual objects. For example, participants in seven pairs tried to draw on other individuals while using Skype (using either the HoloLens or the tablet), and participants in six pairs placed holograms on top of their partner or in front of their face (e.g., Figure 2b).

> *"P8-A: I put a cat on your head.*
> *P8-B: I put the world [a globe] on your head."* (P8)

Such interactions can be problematic either if the other user *can* see the hologram on them (e.g., blocking their vision) or if they *cannot* see it (e.g., if an adversary "*put like a digital sticky note on [the user's] back*" (P4-A)). As we discuss in Section IV-C, participants voiced concrete concerns along these lines during the semi-structured interview phase.

Shooting at Each Other. Echoing observations from Section IV-A regarding participants' assumptions about shared virtual content, we observed participants target each other with virtual objects even when their partner could not see those objects. For example, while using the single-user app RoboRaid, participants in six pairs attempted to shoot each other (or the researchers, who were not wearing HoloLenses). This example raises the question of whether uninvolved bystanders will become unwilling participants to other users' AR experiences, and participants later voiced concerns rooted in not knowing what another user sees (Section IV-C2).

Interfering with Others' Objects. When virtual objects *were* shared, as in the Shared Blocks app, participants sometimes attempted to interfere with their partner's objects. For example, participants in three pairs destroyed structures their partner had built, or stole control of blocks from each other.

> *"P4-B: He's messing with my blocks!*
> *P4-A: I stole his block and I'm like carrying it around."* (P4)

Though these interactions seemed largely experimental in the context of the study, they nevertheless represent potential tensions between people in multi-user AR settings. As we discuss in Sections IV-D and V-A, these tensions raise critical design challenges for multi-user AR systems and applications around object ownership, visibility, and control.

Using Virtual Objects as Physical Barriers. Building directly on an observation from Section IV-A above, we noted that participants sometimes used the opacity of virtual objects to their own advantage. For example, one participant crawled behind a pile of virtual blocks to hide from his partner and then popped out, as shown in Figure 3. Thus, AR enables new risks between multiple people interacting in the *physical* world, not just in the digital world.

Fig. 3: This participant leveraged the opacity of virtual objects in the Shared Blocks application to hide from his partner behind a pile of blocks and pop out.

Actions Triggered by Commands from Others. When multiple people use AR systems in close proximity, their commands may interfere with each other. Participants in two pairs experienced either gestures or voice commands from their partner (or the researchers) triggering actions on their own device. For example, when a researcher instructed P7-B to say the voice command "next", the participant remarked that the instruction actually triggered the command. In another case, P6-A observed her HoloLens react to a hand gesture from her partner. Although these interactions happened accidentally during the study, they could also be exploited adversarially by people in close proximity to an AR user.

Collaboration. Finally, we emphasize that although in this section we focused on tensions or threats between AR users or physically proximate people, multi-user AR interactions can also enable cooperation, as discussed in Section II. Indeed, participants sometimes worked collaboratively in our study. For example, five pairs worked together to build structures such as towers or forts in Shared Blocks. Thus, a challenge for multi-user AR platforms is to enable these types of collaborative interactions between benign users, while also protecting users from potential threats from less cooperative users.

C. End User Concerns

In Sections IV-A and IV-B above, we observed participants' expectations of and behaviors with the HoloLens, and we hypothesized risks that might stem from these experiences. In this section, we shift focus to our second research question (RQ2), uncovering specific risks that our participants surfaced during semi-structured interviews, when presented with several adversarial scenarios and after having experienced a real AR technology. Recall from Section III-D5 that we asked participants to consider specific adversarial scenarios involving other users and untrusted applications. We did not, however, prompt them with any specific risks that might stem from these scenarios. Our goal was not to determine the set of adversaries that participants might be concerned about, but rather to identify the spectrum of specific risks that they believe could arise in emerging AR ecosystems.

By providing participants with several open-ended adversarial scenarios, we enabled them to think about concrete situations in which misuse or harm might arise, and allowed them to identify the potential outcomes of those situations that they would find most concerning. For example, while we prompted participants to consider harassment from other users (recall Section III-D5), we explicitly did not prompt them to consider specific outcomes such as physiological harm (as discussed in Section IV-C1), and hence all mentions of such harms arose organically from participants.

We organize the rest of this section around the types of concerns that participants raised in response to our adversarial scenarios, rather than around the scenarios themselves, since many concerns arose in response to multiple scenarios. We note inline any situations in which a particular concern referred to a specific scenario. Table IV lists our top-level hierarchical codes that capture these concerns, formed by clustering individual codes for similar, thematically-related concerns. Some of these concerns suggest novel risks and challenges for multi-user AR systems (as we further expand upon in Sections IV-D and V-A), while others validate and add richness to theoretical concerns raised by prior works considering security for single-user AR settings.

1) The Risks of Immersion

A unique property of emerging AR systems is the ability to provide immersive experiences that directly impact users' perceptions and actions within the physical world. Indeed, many of the assumptions and behaviors discussed in Section IV-A stemmed from this sense of immersion, which — despite the HoloLens's technical limitations — raised concerns.

> *"This could go really wrong... much more realistic than I thought it would be... When that world can mesh seamlessly with a normal place, that's odd... You're getting closer and closer to something that could be kind of — evil's not the right word, but that could just be a little socially uncomfortable."* (P5-B)

More concretely, our participants identified a few specific risks that might arise from immersive experiences gone wrong.

Physiological Attacks. Participants in all (eleven) pairs considered ways that AR content could physiologically harm users, e.g., by startling them or triggering epileptic attacks.[3] For example, one participant considered the possibility of a malicious user startling the driver of an AR-enabled car:

> *"If they're driving or something... throw a digital object at them, and I could imagine it'd go through the windshield."* (P4-B)

Deception. Nine pairs also expressed concern over the use of holograms to deceive users, likely informed by their observations of HoloLens apps convincingly occluding physical objects as discussed in Section IV-A. For example, P5-B suggested that a malicious app from one company might overlay their brand logo on physical objects from a competing company, as a form of subversive marketing. P9-A and P9-B also considered ways that one user might mislead another by projecting an alternate visual representation of their appearance, or avatar. Furthermore, P4-B discussed ways to hide physical objects with virtual ones:

> *"I'd probably put something like one of the holograms, something boring and innocuous, on top of something like their car keys or their wallet. I imagine it's kind of like... there's physical clutter, you just wouldn't look underneath it."* (P4-B)

Others considered physical consequences that might stem from deceptive holograms, likely informed by their own tendencies to treat virtual objects as extensions of the physical world, discussed in Section IV-A.

> *"P11-B: I think what's going to be really interesting is when we start getting to the point in animation in this when it's getting hard to distinguish real versus fake. Like if you're walking down the street and there's an open manhole cover in front of you — P11-A: Will you think it's the real thing? P11-B: Yeah exactly! And maybe it's already there, and you just see it in your periphery, maybe you do think it's open. Or maybe there's a real manhole cover in front of you and you think it's fake and you don't need to actually dodge it."* (P11)

The above risks are particularly unique to immersive AR environments, where virtual content can lead to serious physical discomfort or harm. These risks may arise in single-user contexts, e.g., from buggy or malicious apps, or they may arise in multi-user interactions (as we saw foreshadowed in the interactions between our participants). In single-user contexts, these risks further support existing efforts to prevent misbehaving AR apps from generating undesirable output (e.g., [26]); in multi-user contexts, these risks raise new defensive challenges, as we discuss further in Sections IV-D and V-A.

2) Unwanted Virtual Content

Whereas the aforementioned concerns largely stem from the immersive potential and physicality of AR, participants also expressed concern about unwanted virtual content more generally. Though such concerns about unwanted content (e.g., ads) may also arise with more traditional technologies (e.g.,

Category of Concerns	Number (of 11 pairs)
(IV-C1) Physiological Attacks	11
(IV-C1) Deceptive Holograms	9
(IV-C2) Virtual Clutter	8
(IV-C2) Obstruction of Virtual Objects	2
(IV-C2) Inappropriate Content	6
(IV-C2) Advertisements	6
(IV-C3) Bystander Privacy	8
(IV-C3) Privacy from Invasive Applications	10
(IV-C4) Displaying Content on People	9
(IV-C4) Obscurity of Other Users' Actions	8

TABLE IV: Concerns raised by participant pairs during semi-structured interviews.

[3] Such concerns have already manifested even with non-AR technology, e.g., a recent case of a reporter targeted with a seizure-inducing tweet [6].

smartphones), the fact that such content might be overlaid continuously on a user's view of the physical world, rather than confined to a small screen, raises new challenges. As above, defenses must consider — and may differ between — both single- and multi-user AR contexts, as well as adversaries including malicious or buggy applications and other AR users.

Virtual Clutter. Eight pairs worried about becoming overwhelmed by virtual objects (which some experienced directly while using the HoloLens), or popups. For example, combining the experiences of using blocks to obscure each other's view in Shared Blocks and seeing an animated virtual monkey eating pizza in the shell, P10-B raised the potential for spamming someone with annoying holograms:

> *"Then there's the situation where someone puts way too many holograms and keeps like placing pizza monkeys... that would be kind of annoying."* (P10-B)

Obstruction of Virtual Objects. Virtual objects can be used to obstruct not only physical objects, as described above, but also other virtual objects. Two pairs were concerned about this capability. For example, P5-A became annoyed with a virtual chirping bird in the shell, and considered how a malicious user might prevent someone from removing such an object by hiding it among other virtual objects.

> *"I thought of trying to hide [virtual] content from somebody... You put like an annoying little bird and hide him in blocks."* (P5-A)

Inappropriate Content. Participants in six pairs discussed unsolicited or inappropriate AR content, in some cases based upon capabilities showcased in the HoloLens apps used in the study, such as Skype's free-drawing feature.

> *"For example, graffiti... people would be drawing penises everywhere."* (P11-A)

Advertisements. Six pairs expressed concern over unwanted ads. Though this concern arose in the context of asking participants to consider risks with untrusted applications, we note that we did not prime participants to think about ads in particular (nor did any of the HoloLens activities include ads).

3) Privacy

Another general class of concerns arose around privacy — privacy from untrusted applications and other users, as well as privacy of both virtual and physical world information.

Privacy for Bystanders. Eight pairs raised concerns about privacy for bystanders of users with AR devices. Though these concerns echo prior work [15], we note that this prior work studied individuals who did not necessarily have personal AR experience, and who only observed nearby users wearing a mock-up AR device. In contrast, our study design allowed participants to raise concerns informed directly by their *own* experiences using a real, immersive AR device.

Indeed, participants voiced concerns about how an AR device could be used not only to sense information about them as a bystander ("*get their weight, their measurements, their eye color*" (P11-B)), but also to visually augment that sensor data with sensitive information drawn from elsewhere.

> *"If I felt like they had an application that was recognizing me and saying who I was and what my net worth was and where I lived and all that stuff, that would make me uncomfortable."* (P7-B)

P11-A noted that these concerns can arise even if one trusts the AR user, due to *"hackers"* or over-permissioned apps.

Four pairs mentioned ways in which they might change their own behaviors in response to the presence of nearby AR users, suggesting the risk of a "chilling effect" — for example, by becoming "*more conscious*" of what they said or trying to "*appear more composed*" (P4-B). Two pairs also suggested ways to mitigate their privacy concerns, by requiring that friends remove their devices in the participant's home or mandating manufacturer-enforced recording bans — echoing countermeasures explored in prior work (e.g., [38]).

Privacy for AR Users from Invasive Applications. While privacy concerns around AR have often been discussed in the context of bystanders (e.g., echoing early concerns with Google Glass [42]), significant privacy concerns also arise for AR users themselves. Indeed, ten pairs voiced concern about invasive apps compromising their physical-world privacy. These concerns involved AR applications' abilities to both capture visual information about the user's physical surroundings directly (e.g., seeing credit card numbers) as well as behavioral information about the user (e.g., pulse and eye tracking enabling sensitive inferences).

> *"There's all kinds of really subtle things that an AR headset would be able to tell about you that in an advertisement sense would be really powerful. So to have a marketer have knowledge of like 'you have a crush on this person because you can't stop looking at them' is pretty scary."* (P5-B)

These concerns further support the need for solutions to restrict sensor data available to AR apps, already explored in prior work (e.g., [16, 23, 36, 38, 45]), to protect the privacy of both bystanders and AR users themselves.

Private Holograms. Finally, when we asked participants explicitly about scenarios in which shared or private AR experiences would be useful, they had concrete ideas for both use cases. For example, P6-A mentioned private use cases like "*porn*" or "*Skyping a friend*" as well as shared use cases like "*creating games and art together*". Participants often implied that their private use cases should be hidden from other users:

> *"If I were navigating somewhere, I'd want to be able to keep that sort of thing private."* (P4-B)

Though participants did not voice as an explicit "concern" the idea of someone else seeing their private holograms, their desires for private content within AR suggest that multi-user AR platforms must protect that content. We further discuss challenges with managing shared and private virtual content in multi-user AR interactions in Sections IV-D and V-A.

4) What Other AR Users See

Concerns arose for participants regarding not only virtual content on their own devices, but also the virtual content that

others can see.

Displaying Content on People. Participants worried about the type of virtual content that other AR users might overlay on top of them or other nearby people. A common concern (nine pairs) was the prospect of someone using AR to modify another person's appearance — a concern potentially informed by their attempts to visually modify each other while using the HoloLens (e.g., placing holograms on each other's heads), as described in Section IV-B.

> *"Can you do that with HoloLens, change somebody? Like you're looking at somebody and you can change what they look like? It's kind of like you would do with Snapchat... That gets kind of psychologically wee-ooh-aah... Can you imagine people married, and they imagine somebody else?"* (P6-A)

Further, participants in two pairs were concerned about the potential for AR users to display personal ratings around others, or to have *"social scores floating by them"* (P1-B). P1-B also considered the idea of displaying embarrassing facts above a person's head that nearby users could see.

Though augmenting people with virtual content is promising to explore (e.g., displaying the names and affiliations of people at an academic conference, or modifying people's appearances with permission during a costume party), our findings suggest that they should also be designed carefully to consider potential misuse or unexpected social consequences.

Obscurity of Other Users' Actions. When virtual content is not shared between multiple AR users, or when a non-AR user interacts with an AR user, multiple people may see different views of the same physical space. Particularly for emerging AR devices like the HoloLens, which provide a private heads-up display for a single user (unlike AR content displayed in a smartphone app), how — and even whether — these views differ can be hidden from other people.

Indeed, participants in eight pairs discussed the assumptions they might make, and the social challenges that might arise, if they could not tell what an AR user was doing.

> *"If they were just kind of staring off into space I'd assume they were checking their email or watching a YouTube video or something like that, but if they were staring at someone, or like staring at different people, maybe something more malicious."* (P4-A)

Both of the above classes of concerns (overlaying on people and the obscurity of an AR user's actions) may manifest for bystanders as well as other AR users seeing different virtual content. However, we observe that multi-user systems have an opportunity to help *mitigate* these concerns. For example, future work might explore mechanisms for AR users to provide some degree of transparency about their actions to other AR users, without leaking private information (e.g., the same way putting down a physical phone signals that one is paying attention). Additionally, our findings suggest that providing users with recourse over unwanted augmentations "attached" to them in some way may ease concerns.

5) Lack of Concern

As discussed in this section, participants raised many concerns surrounding AR technologies. However, we also observe that some participants were notably unconcerned about the potential for AR to be abused by other users or applications.

> *"I don't think I'm really that worried about things that people would do to me. AR wouldn't really be somewhere that I'd feel unsafe... especially because you can see the real world."* (P8-A)

Some users may not view risks of AR as impediments to adoption, and indeed there may be circumstances in which this lack of concern is warranted (e.g., when interacting with trustworthy users or well-vetted apps). Nevertheless, where there are disconnects between users' mental models of AR and what is technically possible, there may be an opportunity for researchers and developers to help shape users' expectations and take measures to protect users from abuse.

Further, from understanding *why* users might lack concern, we can develop an intuition for possible defensive measures. For example, the lack of concern in the above quote rests on the ability to "see the real world" — emphasizing the value, from a defensive perspective, of enabling users to reliably perceive the physical world (either at all times, on demand, or when a possible security situation arises).

D. Challenges for Multi-User AR

Above, we presented a rich variety of concerns our participants raised about risks that may arise in both single- and multi-user AR interactions. Indeed, prior works have identified some of these risks and explored defensive strategies to protect users and bystanders of single-user AR systems. However, our findings suggest that many of these risks can also arise due to other, adversarial AR users — and, as we discuss in Section V-A, defensive techniques designed for single-user systems may not translate well to multi-user AR settings.

In this section, we thus return to our third and final research question (RQ3): what new challenges will arise when considering defensive strategies for *multi-user* AR systems? Although we explore this question in greater depth in Section V-A, we found that our participants presented valuable perspectives to guide this discussion. In particular, we highlight key tensions that arose surrounding *ownership* and *access control*.

Ownership of Virtual Objects and Physical Spaces. By definition, multi-user AR systems allow multiple users to interact with shared virtual content. Determining the precise nature of this sharing raises questions such as: *what* content created by a given user is shared with *whom*, and *how* can those other users interact with this content?

In the least restrictive case, all users could create virtual objects and expose them to other users, and freely view and interact with the objects created by other users (as in our Shared Blocks app, for example). However, it is precisely the potential for unrestricted interactions that appears to form the foundation of many of our participants' concerns.

> *"It feels like the kind of experience where I'd feel powerless very quickly... if somebody started making all of my blocks or all of my things disappear,*

or started putting a bunch of windows in my face, I would feel so powerless about what to do." (P5-A)

In particular, the above sentiment highlights an important desire expressed by many participants — a desire for *ownership* over their AR environments, including ownership over:

- *Virtual objects* perceived as belonging to the user. For example, recall from Section IV-B that one user stole a block created by his partner, and others destroyed block structures built by their partners. Participants' reactions often (seven pairs) suggested a sense of ownership over their own blocks. Recall also from Section IV-C3 some participants' desires for private virtual content (e.g., while navigating somewhere).
- *Personal space*. The above quote suggests that users may desire not only control over their virtual objects but also control over their *physical personal space* (e.g., to prevent objects from appearing in their face). In AR, virtual objects may feel as though they are physically infringing on the user's personal space or may directly impact their perception of the physical world. When considering multi-user systems, a variety of concerns from Section IV-C, ranging from virtual clutter to socially uncomfortable overlays, are intimately tied to the ability of misbehaving users to place unwanted virtual objects in the environments of victim users.

Access Control. The above perspectives raise a key challenge: how can multi-user AR systems give users control over their virtual objects and physical spaces, to prevent undesirable interactions with other users? While we step back and discuss this question further in Section V-A, many participants arrived at this question — and possible answers — on their own, as a result of their HoloLens experiences and general concerns.

Edit Permissions. Five pairs expressed a desire for edit permissions, i.e., mechanisms to prevent other users from freely creating, changing, or deleting objects in their view.

> *"If access to apps was not controlled, then anyone could introduce any app and just interrupt your environment at any time. So for example you're wearing this and you're trying to just navigate the streets without interruption, and someone decides to drop a dragon in the street in front of you."* (P11-A)

View Permissions. Participants in nine pairs also discussed a need for view permissions on virtual objects, to prevent other users from seeing their own private content. The perceived appropriateness of shared or private experiences was often highly contextual — for example, some individuals preferred primarily private content.

> *"Very case by case. Definitely would want an opt-in system, like 'I want to share this object', because I think there's a lot more stuff I'd rather keep [private]. Like 9 times out of 10 I'm not showing people stuff on my phone. Fewer cases where I share stuff. Definitely want, like, tap-to-share."* (P4-B)

Others preferred primarily shared experiences.

> *"I'd like to think that predominantly the reality was shared, and then you had the option to not share if you wanted to, but I would like to think that the default would be like 'hey we're all in the same reality'... And I think that it would actually further the adoption of the technology if people felt like it was a more communal experience as opposed to the haves and have-nots."* (P9-A)

Specific Access Control Mechanisms. In terms of *how* users should manage such edit and view permissions, some participants suggested concrete mechanisms to support explicit sharing decisions (e.g., "*tap-to-share*" from P4-B, above).

> *"It would be really interesting if... it's like 'anything you put on the purple wall is shared'. So then I could have my own environment over here and I could be working and I could be like 'hey check this out' and I throw it up on the purple wall, and then [P8-B] can see it."* (P8-A)

Participants also hypothesized visual aids to help them understand which of their objects are shared:

> *"The color of the window or the adjustable [object bounding boxes] or something — if it would be red for private ones that other people couldn't see and green for public ones that other people can see, instead of I think everything is blue right now, that would be super useful."* (P1-A)

While these mechanisms are by no means the only possible solutions, they provide starting points. Further, the fact that our participants came up with concrete access control mechanisms organically, without being asked to think about such mechanisms, suggests that they valued access control as a design objective. As we discuss next, emerging multi-user AR apps and platforms *must* consider and address these questions.

V. Discussion

Our results — the exploration of user expectations, behaviors, and concerns with a real AR device — allow us to draw broader lessons and recommendations to inform the design of emerging AR technologies, which we present below. We also identify limitations of our study and avenues for future work.

A. Security and Privacy Design Challenges for Multi-User AR

Our findings provide a foundation for understanding and addressing security and privacy for multi-user AR systems — a space that has remained until now unexplored. Below, and continuing to answer RQ3, we identify key design challenges drawn from these findings.

Controlling Access to Personal Objects. Participants desired both view and edit permissions, to restrict others from seeing or modifying their personal holograms (IV-D). While some considered how an AR system might support this control (e.g., "*tap-to-share*" from P4-B), determining appropriate mechanisms remains an open question. This challenge is further complicated by the fact that different users will place differing levels of importance on shared and private experiences (IV-D).

Preventing Unwanted Content from Other Users. The ability for a user to prevent other users from sharing unwanted

content is also critical. Many of our participants' concerns, such as virtual clutter and inappropriate content (IV-C2), were rooted in a lack of such control. However, as above, AR systems will need to determine appropriate mechanisms that account for diverse user sharing preferences.

Negotiating Access to Other Users' Content. Users will also require mechanisms to easily *initiate* sharing requests. If not carefully designed, such mechanisms could (for example) result in a user spamming a victim with requests or accidentally sharing content with the wrong user. One approach may be to leverage a user's physical environment (e.g., "*anything you put on the purple wall is shared*" (P8-A)).

Navigating Partially Shared AR Environments. Users may make different choices in terms of what they share, with multiple interacting users seeing different (possibly overlapping) sets of virtual content. As we saw (IV-A), incorrect expectations of sharing can leave users vulnerable to confusion or harm. AR systems thus have an opportunity to help users better understand what content is shared with whom.

Designing Access Control UIs. The above challenges will all require AR systems to instantiate access control mechanisms with careful UI design, to ensure that the mechanisms can appropriately assist users. While we can draw initial ideas from our participants, such as objects with different colored borders indicating whether they are shared or private (IV-D), access control UIs for multi-user AR remain an open area of study.

Managing Personal Space in AR. While the above challenges involve control over virtual objects, recall from Section IV-D the equally important need to provide users with control over their *physical* personal spaces. Addressing these concerns raises the fundamental challenge of defining personal space in AR, and determining how to best manage the personal spaces of multiple users who may cross paths.

Insufficiency of Single-User Defenses. The above challenges highlight a fundamental tension of multi-user AR systems between supporting flexible shared experiences and preventing unwanted interactions — challenges that may require novel defensive solutions where existing single-user defenses prove insufficient. For example, prior works have proposed mechanisms to prevent undesirable application output in single-user AR contexts (e.g., [26]) and to protect sensitive information from invasive applications (e.g., [16, 23, 36, 45]). However, if applied naively to multi-user systems, the above defenses may lead to unexpected conflicting views or inconsistent application states that impede desirable interactions between users.

B. Grounding Concerns in User Experiences

When considering emerging technologies that are just beginning to gain traction, it is critical to understand the expectations, desires, and potential interactions of end users. While others have conceptually explored the security and privacy challenges presented by emerging single-user AR systems, we find that our study of real users engaging with multi-user AR devices both illuminates new challenges (discussed above) and enriches concerns raised in prior works.

A wide variety of concerns emerged for our participants in response to even limited exposure to a sophisticated-yet-imperfect AR device, when prompted by our adversarial scenarios. Understanding how users envision risks might arise can inform defensive directions previously based only on conceptual risk assessments. We give two examples. First, prior work proposed a framework to enforce policies that constrain virtual content displayed by AR applications [26], deriving potential policies from several sources (e.g., the HoloLens developer guidelines). Our findings can help expand and enrich this set of policies based on the concerns of real users. As another example, while past work proposed techniques for bystanders to prevent nearby AR devices from recording them [38], our participants' concerns about unwanted holographic overlays on people suggest an opportunity to expand these techniques to also prevent nearby AR devices from *overlaying* on others.

C. How These Concerns Might Arise in Practice

Although immersive AR technologies are still quite young, we now reflect upon ways in which our participants' concerns might eventually arise in future AR ecosystems, given the variety of desirable AR use cases being explored. We briefly consider three scenarios in which these concerns could arise, in the absence of appropriate defensive measures.

AR-assisted Driving. Both industry (e.g., [5, 28]) and research efforts (e.g., [7, 41, 47]) continue to explore opportunities for AR-assisted driving (such as tools that overlay speed and braking information of nearby vehicles). Given the safety-critical nature of driving, malicious or buggy AR content could greatly endanger the driver or others nearby. For example (as one participant noted), a digital object that appears as though it was thrown through the windshield could startle the driver. As another example, a deceptive application might misrepresent real-world information, e.g., by occluding pedestrians, changing the values on speed limit signs, or presenting false information about the speeds of nearby vehicles.

Shared AR Art. AR could enable a unique medium of artistic expression, where content creators can layer publicly viewable, digital art or graffiti atop the physical world without modifying the world itself. Ideally, different users within the same physical space could subscribe to their favorite artists for carefully-curated experiences. However, in the absence of an appropriate sharing protocol or access control capabilities, viewers may be subjected to visual spam or inappropriate content from misbehaving parties, with little recourse beyond simply shutting off their application. These concerns were held by many participants, and we have indeed begun to see precursors of such issues already with Snapchat [27].

AR in Schools. Prior work has explored AR as a tool for mathematical education [24], and in future classrooms of all ages, we might see AR used for other educational purposes. However, left unchecked, this technology could manifest as another vector for bullying and abuse among youth. For example, our participants grew concerned about digital content being overlaid on people. An AR application might be used to place a virtual "kick-me" sign or other malicious object on a

victim, and without adequate control over his or her personal space, the victim may have no recourse to remove it or prevent others from seeing it.

D. These Concerns Manifest in Current-Generation AR

The concerns raised in Section IV may seem like issues only for future-generation AR technologies, and indeed we began this work with that assumption. However, our findings suggest that these concerns are in fact imminent, even for today's imperfect AR technologies. That is, our participants' behaviors and interactions demonstrated that the HoloLens — despite its clear limitations — is *already* sufficiently immersive to blur the line between physical and digital experiences, and to elicit serious concerns. For these concerns to manifest as real threats in the AR ecosystem, we need only see an increase in adoption by users and app developers, not a fundamental shift in the underlying technologies.

E. Limitations

Finally, we note several limitations of our study. First, our study was qualitative, and thus we cannot draw quantitative conclusions or generalize our results to a broader population. Instead, the goal of a qualitative study is to surface a broad set of themes — in this case, security and privacy issues around emerging AR technologies. We also do not evaluate how *likely* participants believe specific risks are, focusing instead on their breadth of concerns. Future work should consider studying these questions in a larger-scale quantitative study.

Our study is also likely influenced by our choice of AR technology, the HoloLens. We chose the HoloLens because it is one of the most immersive AR devices commercially available. Though some of our findings are thus HoloLens-specific (e.g., reactions to opaque holograms), they raise lessons that extend to AR technologies more generally. Additionally, recall that participants' expectations were often rooted in their treatment of AR as an extension of the physical world (IV-A). While we center our discussion on physically co-located interactions, future work should also explore how these assumptions do (or do not) change for users engaged in remote interactions.

Though we aimed to recruit diverse participants, our participant pool was likely biased towards people who wanted to try the HoloLens, and who may be more tech-savvy, more likely to be early technology adopters, and more positively disposed towards the technology. Though future work may wish to consider other groups (e.g., people *disinclined* to use AR technology), our results highlight important security and privacy challenges that emerging AR technologies will raise.

Users may behave differently after extended experience with an AR device than during a ninety-minute session. In our work, we aimed to study users' *initial* expectations and experiences, unhampered by pre-existing knowledge that might constrain a more experienced user's perspective. However, these findings may not generalize to more experienced users, and as these technologies become more widely used, future work should study longer-term users' experiences and concerns.

VI. Conclusion

In this work, we identified the fundamental need to explore the security, privacy, and safety challenges of emerging single- and multi-user AR technologies, grounded in the experiences of end users. Through a qualitative lab study with 22 participants (11 pairs), combining hands-on activities with semi-structured interview questions, we studied the expectations, interactions, and concerns of users engaging with the Microsoft HoloLens, an immersive AR headset. We found that participants were easily immersed in HoloLens experiences, treating virtual objects as real despite nontrivial limitations of the current technology; that participants raised a variety of concerns around misuse by multiple actors, including other users and applications; and that multi-user interactions raised fundamental tensions around access control for virtual objects embedded into shared physical spaces. Our findings give us the opportunity to draw broader lessons and suggest key design challenges for future AR technologies, including previously unexplored multi-user issues. Our work thus lays a foundation for understanding and addressing the security, privacy, and safety risks that emerging AR technologies will present.

Acknowledgements

We are especially grateful to our study participants. We thank Camille Cobb, Melody Kadenko, Shrirang Mare, and Lisa Merlin for piloting our study, and we thank Greg Akselrod and Steffi Svendsen for helping inspire this study through their HoloLens experimentation. We thank Eric Zeng for feedback on user study design and analysis, and we thank him as well as Lucy Simko and Niel Lebeck for helpful feedback on earlier drafts. Finally, we thank our anonymous reviewers as well as our shepherd, Lujo Bauer, for their valuable suggestions and guidance. This work was supported in part by the National Science Foundation under Awards CNS-1513584, CNS-1565252, and CNS-1651230.

References

[1] AR Studio. https://developers.facebook.com/products/camera-effects/ar-studio/, 2017.
[2] ARKit. https://developer.apple.com/arkit/, 2017.
[3] Tango. http://get.google.com/tango/, 2017.
[4] World Lens, 2017. https://questvisual.com/.
[5] E. Adams. Drive a car like you'd fly an F-35 with augmented reality. Wired, Feb 2017. https://www.wired.com/2017/02/drive-car-like-youd-fly-f-35-augmented-reality/.
[6] T. M. Andrews. Tweet that sent journalist Kurt Eichenwald into seizure considered 'deadly weapon' in indictment. Washington Post, Mar. 2017. https://www.washingtonpost.com/news/morning-mix/wp/2017/03/22/tweet-that-sent-journalist-kurt-eichenwald-into-seizure-considered-deadly-weapon-in-indictment/.
[7] K. Bark, C. Tran, K. Fujimura, and V. Ng-Thow-Hing. Personal navi: Benefits of an augmented reality navigational aid using a see-thru 3D volumetric hud. In

Proceedings of the 6th International Conference on Automotive User Interfaces and Interactive Vehicular Applications, AutomotiveUI '14, New York, NY, USA, 2014. ACM.

[8] A. Butz, C. Beshers, and S. Feiner. Of vampire mirrors and privacy lamps: Privacy management in multi-user augmented environments. In *Proceedings of the 11th Annual ACM Symposium on User Interface Software and Technology*. ACM, 1998.

[9] A. Butz, T. Hollerer, S. Feiner, B. MacIntyre, and C. Beshers. Enveloping users and computers in a collaborative 3D augmented reality. In *Proceedings of the 2nd IEEE and ACM International Workshop on Augmented Reality*. IEEE, 1999.

[10] K. Charmaz. *Constructing Grounded Theory*. Sage Publications Ltd, second edition, 2014.

[11] J. Cohen. A coefficient of agreement for nominal scales. *Educational and Psychological Measurement*, 20(1), 1960.

[12] L. D'Antoni, A. Dunn, S. Jana, T. Kohno, B. Livshits, D. Molnar, A. Moshchuk, E. Ofek, F. Roesner, S. Saponas, M. Veanes, and H. J. Wang. Operating system support for augmented reality applications. *Hot Topics in Operating Systems (HotOS)*, 2013.

[13] J. A. de Guzman, K. Thilakarathna, and A. Seneviratne. Security and privacy approaches in mixed reality: A literature survey. *arXiv preprint arXiv:1802.05797*, 2018.

[14] N. Dell, V. Vaidyanathan, I. Medhi, E. Cutrell, and W. Thies. Yours is better!: Participant response bias in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2012.

[15] 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 32nd Annual ACM Conference on Human Factors in Computing Systems*, 2014.

[16] L. S. Figueiredo, B. Livshits, D. Molnar, and M. Veanes. PrePose: Security and privacy for gesture-based programming. In *IEEE Symposium on Security and Privacy*. IEEE, 2016.

[17] J. L. Fleiss, B. Levin, and M. C. Paik. *Statistical Methods for Rates and Proportions*. John Wiley & Sons, New York, 3 edition, 2003.

[18] E. Gaebel, N. Zhang, W. Lou, and Y. T. Hou. Looks good to me: Authentication for augmented reality. In *Proceedings of the 6th International Workshop on Trustworthy Embedded Devices*. ACM, 2016.

[19] B. G. Glasser and A. L. Strauss. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Aldine Publishing Company, Chicago, 1967.

[20] G. Guest, A. Bunce, and L. Johnson. How many interviews are enough? An experiment with data saturation and variability. *Field Methods*, 18, 2006.

[21] HoloLens hardware details, 2017. https://developer.microsoft.com/en-us/windows/mixed-reality/hololens_hardware_details.

[22] HoloLens, 2017. https://www.microsoft.com/microsoft-hololens/en-us.

[23] S. Jana, D. Molnar, A. Moshchuk, A. M. Dunn, B. Livshits, H. J. Wang, and E. Ofek. Enabling fine-grained permissions for augmented reality applications with recognizers. In *USENIX Security*, 2013.

[24] H. Kaufmann and D. Schmalstieg. Mathematics and geometry education with collaborative augmented reality. *Computers & Graphics*, 27(3), 2003.

[25] K. Lebeck, T. Kohno, and F. Roesner. How to safely augment reality: Challenges and directions. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications*. ACM, 2016.

[26] K. Lebeck, K. Ruth, T. Kohno, and F. Roesner. Securing augmented reality output. In *IEEE Symposium on Security and Privacy*. IEEE, 2017.

[27] L. Matney. Jeff Koons' augmented reality Snapchat artwork gets 'vandalized', Oct. 2017. https://techcrunch.com/2017/10/08/jeff-koons-augmented-reality-snapchat-artwork-gets-vandalized/.

[28] M. May. Augmented reality in the car industry, Aug. 2015. https://www.linkedin.com/pulse/augmented-reality-car-industry-melanie-may.

[29] T. Merel. The reality of VR/AR growth, 2017. https://techcrunch.com/2017/01/11/the-reality-of-vrar-growth.

[30] Meta, 2017. https://www.metavision.com/.

[31] M. R. Morris, A. Cassanego, A. Paepcke, T. Winograd, A. M. Piper, and A. Huang. Mediating group dynamics through tabletop interface design. *IEEE Computer Graphics and Applications*, 26(5), 2006.

[32] T. Moynihan. It's a good thing the F-35's $400k helmet is stupid cool. Wired, Jun 2016. https://www.wired.com/2016/06/course-f-35-comes-400000-augmented-reality-helmet/.

[33] T. Olsson, P. Ihamäki, E. Lagerstam, L. Ventä-Olkkonen, and K. Väänänen-Vainio-Mattila. User expectations for mobile mixed reality services: an initial user study. In *European Conference on Cognitive Ergonomics: Designing beyond the Product—Understanding Activity and User Experience in Ubiquitous Environments*. VTT Technical Research Centre of Finland, 2009.

[34] T. Olsson, E. Lagerstam, T. Kärkkäinen, and K. Väänänen-Vainio-Mattila. Expected user experience of mobile augmented reality services: a user study in the context of shopping centres. *Personal and Ubiquitous Computing*, 17(2), 2013.

[35] T. Olsson and M. Salo. Narratives of satisfying and unsatisfying experiences of current mobile augmented reality applications. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2012.

[36] N. Raval, A. Srivastava, A. Razeen, K. Lebeck, A. Machanavajjhala, and L. P. Cox. What you mark is what apps see. In *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 2016.

[37] F. Roesner, T. Kohno, and D. Molnar. Security and privacy for augmented reality systems. *Communications of the ACM*, 57(4), 2014.

[38] F. Roesner, D. Molnar, A. Moshchuk, T. Kohno, and

H. J. Wang. World-driven access control for continuous sensing. In *ACM Conference on Computer & Communications Security*, 2014.
[39] S. D. Scott, M. S. T. Carpendale, and K. M. Inkpen. Territoriality in collaborative tabletop workspaces. In *Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work*. ACM, 2004.
[40] I. Sluganovic, M. Serbec, A. Derek, and I. Martinovic. HoloPair: Securing shared augmented reality using microsoft hololens. In *Annual Computer Security Applications Conference (ACSAC) 2017*, 2017.
[41] S. Sridhar and V. Ng-Thow-Hing. Generation of virtual display surfaces for in-vehicle contextual augmented reality. In *2012 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*. IEEE, 2012.
[42] J. Swearingen. How the camera doomed Google Glass, Jan. 2015. https://www.theatlantic.com/technology/archive/2015/01/how-the-camera-doomed-google-glass/384570/.
[43] Z. Szalavári, D. Schmalstieg, A. Fuhrmann, and M. Gervautz. studierstube: An environment for collaboration in augmented reality. *Virtual Reality*, 3(1), 1998.
[44] D. Takahashi. Pokémon go is the fastest mobile game to hit $600 million in revenues, 2016. http://venturebeat.com/2016/10/20/pokemon-go-is-the-fastest-mobile-game-to-hit-600-million-in-revenues/.
[45] R. Templeman, M. Korayem, D. Crandall, and A. Kapadia. PlaceAvoider: Steering first-person cameras away from sensitive spaces. In *Network and Distributed System Security Symposium (NDSS)*, 2014.
[46] R. Tilton. Daydream Labs: positive social experiences in VR. Google, Aug. 2016. https://www.blog.google/products/google-vr/daydream-labs-positive-social/.
[47] C. Tran, K. Bark, and V. Ng-Thow-Hing. A left-turn driving aid using projected oncoming vehicle paths with augmented reality. In *5th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, 2013.
[48] J. Vilk, A. Moshchuk, D. Molnar, B. Livshits, E. Ofek, C. Rossbach, H. J. Wang, and R. Gal. SurroundWeb: Mitigating privacy concerns in a 3D web browser. In *IEEE Symposium on Security and Privacy*, 2015.
[49] D. Wagner, T. Pintaric, F. Ledermann, and D. Schmalstieg. Towards massively multi-user augmented reality on handheld devices. In *Pervasive*, volume 2005. Springer, 2005.
[50] Wikitude, 2017. https://www.wikitude.com/showcase/tripadvisor-be-in-the-know/.
[51] N. Yee, J. N. Bailenson, M. Urbanek, F. Chang, and D. Merget. The unbearable likeness of being digital: The persistence of nonverbal social norms in online virtual environments. *CyberPsychology & Behavior*, 10(1), 2007.
[52] K. Yeung. Microsoft partners with Autodesk to bring 3D product design to HoloLens, 2015. https://venturebeat.com/2015/11/30/microsoft-partners-with-autodesk-to-bring-3d-product-design-to-hololens/.

APPENDIX

Below, we describe our study protocol, summarizing each phase of the study in order, and also providing our concrete semi-structured interview questions. We followed this protocol for every interview, only departing under two circumstances:

1) In some situations, if a participant said something particularly vague, we asked them to elaborate or unpack their thoughts more, before resuming with the script. We did not ask leading questions or guide participants towards specific opinions when asking for elaboration. Rather, we simply sought additional clarification on points that participants themselves had already raised.
2) If a participant began discussing thoughts related to an upcoming question in our interview protocol before being explicitly asked that question, we let them continue their train of thought rather than interrupting them. If appropriate in the flow of conversation, we would ask them the corresponding question from our script before resuming with the script as structured below. When this scenario occurred, it typically resulted in a minor re-ordering of General Experience questions within either phase 4 or phase 6. Occasionally, it resulted in the elevation of questions from phase 8 into phase 6.

We note that we specifically did not depart from the below protocol for phase 7 under any circumstances (Security, Privacy, and Other Concerns). To avoid prematurely priming participants to consider adversarial scenarios, we did not ask any questions from phase 7 until the conclusion of all previous phases, regardless of any previous thoughts participants may have discussed that were related to the topics covered in phase 7. Additionally, questions within phase 7 were presented in the same order for every participant pair.

Section III-D of our paper provides an overview of our study protocol. We provide additional details here, with the interview phases numbered below.

1. Overview Explanation. We began each interview by explaining the basics of augmented reality to participants (i.e., applications that overlay digital content directly on a user's perception of the physical world through some sort of device), explaining that they would be using an AR headset called the Microsoft HoloLens, and by providing an overview of our study (described below and also in Section III-D of the paper), before providing participants with consent forms to sign if they wished to participate.

2. Interview: Initial Questions. We asked participants the following questions:

- What drew you to sign up for this study?
- Have you heard of AR before? If yes, what have you heard?
- Have you used any AR applications before?
  - Which ones?
  - On what devices?
- Have you seen other people using AR before? If so, where/when?
  - What about in fiction books, or in film?

3. Activity: HoloLens Tutorial + Shell. We next asked participants to go through the HoloLens tutorial, followed by using the HoloLens shell, as described in Section III-D.

4. Interview: Initial Experience + Brainstorming. We asked the following questions, providing participants with a short period of time to gather their thoughts and take notes on paper after we asked each question, before verbally answering. For each interview phase, we ensured that both participants had an opportunity to speak.

- What do you generally think so far?
- What stood out to you the most?
- What did you like the most about what you've seen so far, or what seemed the "coolest"?
- What bothered you about your experience so far, or what did you find the most frustrating?
- Have you found anything particularly confusing or surprising so far?
- Did you expect that you were both seeing the same holograms?
  - Why or why not?
  - Would you have preferred one way or the other?
- Is there anything else you thought of that we didn't cover?

We then asked participants to think about what kinds of things augmented reality might be useful for, either now or in the future. We asked participants:

- What kinds of situations might you want to use AR in?
- What kinds of things would you want to be able to do with AR applications?

For the above 2 brainstorming questions, we had participants silently think and write down their individual thoughts for approximately a minute or two, after which we asked them to discuss their thoughts with us and with each other.

5. Activity: HoloLens Applications. As described in Section III-D, we uniformly randomized the order in which each pair of participants used three HoloLens applications. Within a given pair, both participants used the same apps at the same times. In Section III-D, we discuss our rationale for uniformly randomizing application order. For each app, we provided participants with basic initial instructions on how to use the app, after which we remained passive observers, only speaking in response to explicit questions from participants directed at us.

6. Interview: General Experience. We asked a similar set of questions as those immediately following the tutorial+shell phase, regarding participants' general experiences, now that they had experienced more HoloLens applications. For these and the below questions, as above, we gave participants a brief period of time to write down notes before verbally answering each question:

- What did you think of your experience overall?
- What stood out to you the most?
- What did you generally like, or what about your experience was the "coolest"?
- What generally bothered you about your experience, or what did you find the most frustrating?
- Did you find anything particularly confusing or surprising?

7. Interview: Security, Privacy, and Other Concerns. For the below topics (as discussed in Sections III and IV of the paper), we emphasize that while we prompted participants to consider a set of possible adversaries and scenarios, we did not mention any specific threats or concerns that might arise from these adversaries or within these scenarios.

Interview: Abuse of AR Technology. We asked participants the following questions:

- Now I want you to imagine you are someone that is trying to prank or troll someone else, like a sibling or friend, or maybe someone you really dislike. Let's say you're both using AR glasses like HoloLens, in a multi-user scenario like we talked about before. What kinds of things might you try to do to mess with the other person?
- Now imagine someone was trying to troll you, or make you have a really bad experience. What kinds of things would you be worried about them doing?

Interview: Untrusted Applications. We asked participants one question regarding applications downloaded from the Internet:

- Imagine you had downloaded some applications from the Internet for an AR headset. Is there anything that you might worry about those apps doing?

Interview: Bystanders. We asked participants a few questions about bystanders to AR technology:

- Imagine you are in public somewhere, like on the bus, on campus, or in a grocery store - think of places you typically go. If you saw someone wearing an AR headset in these types of situations, how would you feel? And what kinds of things would you think the person is doing?
- Would your opinions change if the person is someone you know vs. a stranger?
- Would your opinions change if the person was in a more personal space, like your home, rather than in public?
- How would you feel if you weren't wearing an AR headset, but you were trying to talk or interact with someone who was wearing one?

8. Interview: Multi-User Experiences. Finally, we asked participants to consider multi-user AR experiences:

- You've seen different scenarios now; sometimes you could see the same holograms (like the multiplayer game) and sometimes you couldn't (like the robot shooting game). Did you prefer one over the other?
- Can you think of some scenarios where shared views might be more useful, or scenarios where private views might be more useful?