Ethics Emerging: the Story of Privacy and Security Perceptions in Virtual Reality

Devon Adams
University of Maryland, Baltimore County
adadev1@umbc.edu

Alseny Bah
University of Maryland, Baltimore County
abah4@umbc.edu

Catherine Barwulor
University of Maryland, Baltimore County
barwulo1@umbc.edu

Nureli Musabay
James Madison University
musabanx@dukes.jmu.edu

Kadeem Pitkin
College of Westchester
kpitkin@cruiser.cw.edu

Elissa M. Redmiles
University of Maryland
eredmiles@cs.umd.edu

ABSTRACT

Virtual reality (VR) technology aims to transport the user to a virtual world, fully immersing them in an experience entirely separate from the real world. VR devices can use sensor data to draw deeply personal inferences (e.g., medical conditions, emotions) and can enable virtual crimes (e.g., theft, assault on virtual representations of the user) from which users have been shown to experience real, significant emotional pain. As such, VR may involve especially sensitive user data and interactions. To effectively mitigate such risks and design for safer experiences, we aim to understand end-user perceptions of VR risks and how, if at all, developers are considering and addressing those risks. In this paper, we present the first work on VR security and privacy perceptions: a mixed-methods study involving semi-structured interviews with 20 VR users and developers, a survey of VR privacy policies, and an ethics co-design study with VR developers. We establish a foundational understanding of perceived risks in VR; raise concerns about the state of VR privacy policies; and contribute a concrete VR developer "code of ethics", created by developers, for developers.

1. INTRODUCTION

Virtual Reality (VR) technology aims to create "immersive, interactive, and imaginative" simulations for the user through visual, haptic, and auditory output [14]. The goal of VR is to create an entirely immersive experience that fully transports the user away from reality and into a virtual world [47]. While VR headsets have existed since the 1960s, they are fairly recent to the commercial market [47]: the first headset with fully-realized VR capabilities—the Oculus Rift—became commercially available in 2016. The VR market has been growing ever since, with VR revenue projected to grow from $12B to a $100B in the next five years [31].

VR systems may collect sensitive data such as facial muscle movements, which can be used to discern users' emotions or quality of health, and high-fidelity infrared images of users' environments [35]. Perhaps most uniquely, VR technology can lead to visceral real-world emotional pain caused by virtual crimes (e.g., physical attacks on virtual characters that the VR user feels they embody) [33], can cause seizures [9], and has been used as a medical device, including for PTSD therapy [40]. While prior work has studied user perceptions of privacy and security for augmented reality [1] (AR) [41, 26, 22, 15], as well as for other IoT devices such as drones [7, 10, 8, 48] and health trackers [38, 32, 27, 50, 25, 39], no such similar examination has focused on VR.

By studying VR early in the technology-adoption lifecycle, we have a unique opportunity to understand security and privacy perceptions and practices as they develop. Unlike fitness trackers, for example, which are already widely adopted, VR headsets only recently became widely available for consumer purchase and only 3% of the US population uses VR monthly [42]. Thus, the current users of VR are "innovators", as defined by Diffusion of Innovations theory [43], willing to explore the uncertain, adopting technologies that are not yet socially supported or pervasive. As privacy and security researchers, we rarely have the opportunity to develop mitigations before problems become wide spread. As such, VR presents a unique opportunity for future research and proactive technological and design solutions.

In this work, we use a mixed-methods approach to form a foundational understanding of human-centered privacy and security risks in VR. We conduct semi-structured interviews with VR users (n=10) and developers (n=10); survey the current state of privacy policies for VR experiences (i.e., applications); and conduct a co-design study with VR developers to create a "code of ethics" for development in VR.

In our interviews, we query users' and developers' *information sources* and *concerns*, especially around security and privacy; *knowledge and perception* of data collection; and VR fits into their *social structures*. Highlights of our findings include identifying three domains of VR concern: *well-being*, which encompasses both the physical (e.g., motion sickness, vision damage) and psychological (e.g., intensity of experiences, harassment); *privacy*, primarily data collection; and, to a lesser extent, *security*. We also identify a strong emphasis on community. Users describe the VR community as *exclusive and small*, which consequently makes them feel

[1] AR adds virtual elements to a live view of the real world, may incorporate real-world bystanders into the experience [15], and does not necessarily require the user to wear a headset (e.g., PokemonGo). VR, on the other hand, creates an immersive environment without connection to reality through visual, audio, and haptic experiences transmitted through a VR headset and haptic controllers or even body suits [46].

safe, but wary of the future, when the "general public" can afford to use VR. On the other hand, developers describe the community as *small, supportive, and open*, which facilitates knowledge sharing and learning, including discussion of privacy, security, and other ethics-related topics.

One such privacy topic brought up by the developers was privacy policies. The developers we interviewed viewed privacy policies as a method for achieving transparency around data-collection with end-users. Although prior research suggests that privacy policies may be ineffective for achieving this goal [30, 12, 37], to gain a supplemental, objective, understanding of the state of data collection transparency between users and developers we examined VR privacy policies . We randomly sampled 10% of the applications available for HTC Vive and Oculus (the producers of the VR systems our participants used most). Only 30% of the HTC Vive applications we sampled had a privacy policy posted. And, while 82% of the Oculus applications had a posted policy, only 19% of those policies explicitly mentioned VR or VR data. Thus, even if privacy policies were a good method of developer-user transparency, the current ecosystem of VR privacy policies would not achieve this goal.

Our interview results provide one possible hypothesis for the problematic state of VR privacy policies: a lack of standards for developers. The majority of developers with whom we spoke reported struggling to figure out how best to protect end-users. They cited a lack of guidelines in the community as one of the causes for this struggle. As two developers mentioned, "there are no advisors right now," and "there's a quite a big list of unknowns right now in terms of what's best etiquette for a user and what's gonna keep them the most [safe], comfortable, and satisfied." As a first step toward filling this gap, and better aligning the concerns and desired protections expressed by the VR users and developers, we conducted a co-design study open to 11 online communities of developers. In our study, developers from these communities came together, with our moderation, to create a "code of ethics" for VR development. The resulting code includes 10 principles for development in VR, including principles focused on accessibility, maintenance of safe social spaces, and avoiding causing physical or psychological harm to users.

The relative success of our co-design study, and the sustained views and comments on the document after the study period ended, suggest that collaborative work with developer communities may be an effective method for ensuring end-user protection and more secure applications, even beyond VR. Such collaborative processes may be especially successful in small, open communities such as that described by the VR developers we interviewed. While the close-knit nature of the community described by users and developers has benefits—it elicits the users we interviewed feel safer and appear to support developer learning—it can also lead to the exclusion of certain demographic or social groups, risking the development of a technology tailored toward the needs and interests of only those with enough resources to become early adopters. Finally, our results suggest a number of emerging concerns in VR including harassment, transparency about data collection, and security vulnerabilities, which future work should push to address early, before VR becomes more widely adopted.

2. RELATED WORK

We briefly review prior work on VR risks and potential mitigations and on IoT privacy and security, more broadly.

2.1 VR Risks

VR risks to users fall broadly into three categories: data collection and inferences [35, 41]; physical harms [11, 53]; and manipulation and violation of immersive experiences [29, 24]. VR systems collect haptic, audio, and camera inputs that can be used to infer or even treat medical conditions, enhance simulations, and drive profits [35, 40]. Such information may be collected even when the user believes the system is off, as many headsets are "always on", enabling developers to gain data without the users' knowledge [41]. This data may then be sold to third parties [35] or be leaked through known vulnerabilities [29], which may have consequences such as modifying the quality and pricing of goods or services advertised to users.

Finally, O'brolchin et al. theorize that virtual reality social networks will create a 'global village' with stronger discourse and interaction than is available in current social networks [35]. While enhanced community is a great potential benefit of VR, it also increases the risk of users sharing personal and sensitive information with unknown and untrusted third parties or being harassed. VR also enables virtual crimes (e.g., physical attacks on virtual characters, stealing of digital goods), which prior work has found generate strong emotional reactions similar to real-world crimes [33, 49, 24]. To protect against these threats, early work has explored defenses for VR, including specialized authentication systems for 3D environments [54, 18, 5, 6].

While there has been no systematic exploration of risks in VR, Roesner et al. and Lebeck et al. survey the space of AR threats [41, 26]. They point out similar concerns in AR as listed above for VR, in addition to raising concerns about output security: the integrity of the users' virtual experience. Additional work by Denning et al. investigate raises an additional AR concern: bystander effects—the incorporation of a bystander into the virtual experience. While real-world bystander effects are unlikely to occur in virtual reality, virtual avatar representations of users may become bystanders to other users experiences in VR [15]. Finally, Jana et al. work explores methods for fine-grained permissioning in AR, including the development and evaluation of "privacy goggles" that can help users visualize the kinetic data that AR systems can collect about them [22]. The authors of this prior AR work emphasize the importance of addressing AR threats early, before issues occur [41]; we argue that the same can be said of threats in VR—especially given that the more immersive nature of the VR experience presents uniquely different psychological threats as described above.

A key component to identifying and prioritizing the mitigation of VR risks, and developing legislation and policy protections for VR users, is understanding users' and developers' concerns. Only one piece of prior work, to our knowledge, has explored user privacy and security perceptions around VR: Motti et al. collected online comments about digital glasses and other head-mounted devices (which included a small number of VR headsets) from forums, social media, and various websites [32]. We expand on Motti et al.'s findings, focusing exclusively on VR and collecting more in-depth data than is available through online com-

ments.

2.2 Privacy and Security in IoT

Users' perceptions of privacy and security risks have also been explored in related domains, such as drones and fitness trackers. Prior work has found that people are acutely aware of the privacy and security risks around drones [7, 10, 8] and worry about the potential sale of data collected from their fitness tracking devices [32, 27, 50, 25, 39].

However, despite these concerns, Rader et al. found that fitness tracker users often struggle to consider the broader consequences of inferences that can be made with this data, making it challenging for them to self-manage their privacy around sensor data collection [38]. This finding, together with prior findings that transparent information helps users make more informed decisions [10, 48, 8], underscores the importance of assessing user and developer awareness of risks in VR so that we can increase awareness and provide strategies to mitigate emerging risks.

3. METHODS

In this section we describe our interview methodology and analysis approach, our privacy policy analysis, and our co-design study with VR developers and subsequent trace ethnography analysis. [2] We conclude with a discussion of the limitations of our approach.

3.1 Interview Study

3.1.1 Recruitment

We were interested in studying home consumers of VR and the developers of content for commercially available VR systems. Given the low adoption rate of VR (3%) [42], we do not focus on users or developers for one particular VR platform or application (e.g, Oculus Rift users or VR gamers). We recruited both users and developers by posting advertisements in 17 VR-related Reddit communities, Facebook groups, and online forums (list of communities and advertisement text is included in Appendix A). Participants completed a short screening questionnaire containing demographic questions and asking them to indicate whether they were a VR user or a developer. To verify that users and developers were authentic in their answers, users were required to upload an image of themselves using their VR headset, while developers were required to briefly describe a VR experience they are developing and what language or tools they use to develop.

3.1.2 Protocol

Eligible participants were invited to participate in a 20 minute semi-structured interview via phone, Skype, or Google hangouts, and were compensated with a $15 Amazon gift card for their participation.

We used different protocols for the developers than for the users (see Appendix B for full protocols), however, both protocols covered the same high level topics:

- VR Background. We attempted to capture background information regarding the participants' VR use to better contextualize our findings. This included capturing the VR platform used or developed on (e.g., Oculus Rift, HTC Vive), the VR domain (i.e., what users do with their headsets or the type of experiences developers are creating), participants' goals for using or developing in VR, and evangelizing experiences (i.e., whether the user or developer recommends VR to others).

- Information Sources. For users, how they learned about VR and what heuristics they used to select their VR platform. For developers, how they learned about the possibility of developing for VR and what resources they used to learn necessary development skills.

- Concerns. Our questions about concerns began generally, "Did you have any concerns about starting to [use/develop for] VR? Do you still have concerns?" With follow up questions probing specifically about security concerns or envisioned threats and privacy concerns or threats.

- Data Collection. what data they thought was being or could be collected in VR (for developers what data their experiences collected or could collect), recommendations for others/evangelizing of VR.

Six different researchers conducted the interviews in pairs, researchers of different ethnicities and genders were used to randomize and minimize interviewer biases [36].

3.1.3 Analysis

Each interview was transcribed word-for-word. Then, six researchers reviewed four of the twenty interview transcripts to develop a qualitative codebook. Separate, but similar, codebooks were created for the developer and user interviews. Each interview was double coded: interviews were coded by Researcher 1 and by one of the five other researchers, such that there was a single researcher who had coded every interview for comparison consistency. The researchers achieved an average Krippendorff's alpha of 0.72 across all the transcripts, which is above the minimum suggested threshold for exploratory studies such as this one [28].

3.2 Privacy Policy Analysis

To better understand data collection and transparency between developers and users in VR, we analyzed VR experience privacy policies. To do so, we randomly sampled 10% of the experiences in the "experience stores" for the two commercially available headsets that were used or developed for most by our participants: Oculus Rift/Gear (90 applications) and HTC Vive (50 applications). We labeled the sampled applications for whether they had a posted privacy policy posted and, if so, whether that policy mentioned VR (e.g., VR data, sensors, or experiences). If the policy mentioned VR, we recorded what was mentioned. Three researchers labeled the sample of 140 applications; as the labeling was objective (had a privacy policy or not; mentioned VR or not) we did not double-label.

3.3 Code of Ethics Co-Design Study

A majority of the developers we interviewed mentioned, unprompted, that they wished for an agreed upon standard of practice or "code of ethics" for development in VR. To fill

[2]The user-study portions of our work were approved by our institutional review board.

this gap, we conducted a co-design study in which we invited VR developers and content creators to collaboratively develop a code of ethics for VR development.

3.3.1 Advertisement

To reach developers, we posted in most of the same Facebook, Reddit, and forum communities (11 developer-specific or developer-heavy communities, identified in Appendix A) as we did when recruiting for interview participants. In our post, we briefly described our motivation for our project and then directed readers to the document described below and asked them to help create a VR developer code of ethics (advertisement text is included in Appendix A). We offered a $2 Amazon gift card to any developer who made a meaningful contribution to the document and emailed us about their contribution.

3.3.2 Document Collaboration

To help the developers get started on the code of ethics, we created a starter document in Google Docs [3], a collaborative document editing platform. The document contained seven potential principles such as "Do No Harm" that emerged from our interview results. We provided the following instructions: "We have placed some ideas for a set of standards for ethical development in VR based on our research findings and the thoughts raised by participant in our research. Please feel free to completely rewrite the standards, discuss your changes in the chat, and etc."

3.3.3 Analysis

To analyze the process by which developers collaborated on creating the code of ethics, we use trace ethnography [17]. Trace ethnography is an extension of document ethnography specifically designed for digital environments and has been used to analyze similar online collaborative processes such as Wikipedia editing [17]. We explore which sections of the document were most edited or commented upon, the different roles of those engaged in developing the document, and the process by which consensus was reached. As is typical of ethnographic research, one of the researchers who was trained in ethnography conducted this portion of the analysis.

3.4 Limitations

In qualitative studies, sufficient sample size and participant diversity are necessary to decrease bias and increase the generalizability of findings. In the interview portion of our study, we conducted interviews until new themes stopped emerging and reaching a sample size within qualitative recommendations [16] for exploratory, foundational studies such as ours. We attempted to ensure that our participants were demographically diverse through demographic screening; however due to bias in the demographics of potential participants who signed up for the study and subsequently attended interviews, and the fact that VR users and developers make up less than 3% of the US population, our sample skews male, more Asian, more educated, and young.

Finally, for the co-design portion of our study, we did not control which developers chose to edit our document nor did we collect any information about those who viewed, shared, or edited the document. Our co-design study, and resulting code of ethics document, is thus biased by those who chose to participate. However, when considering our research within the broader context of the VR community, we felt that it was most important to ensure organic, open participation.

[3]https://www.google.com/docs/about/

4. RESULTS

In this section we present the results of our three-part study, beginning with a description of the interview participants and findings, followed by the results of our VR privacy policy analysis and, finally, the results of our code of ethics co-design.

4.1 VR Privacy and Security Perceptions

Overall, we find that developers and users express concerns around three classes of risks: well-being, security, and privacy. These concerns vary by their role (developer or user) and, for about half of them, their experiences in the VR community. Figure 1 summarizes the types of risks that users and developers discussed, as well as the background information about their VR use, goals, and community perceptions that we analyze. Figure 2 summarizes the similarities and differences between user and developer concerns: overall we find that developers focus more on well-being—especially physical and psychological—while users focus more on security; both groups mentioned privacy concerns with near equal frequency and emphasis. Neither group was as concerned about security as about well-being and privacy.

4.1.1 Participant Overview

Participant Pool. 98 potential participants completed our demographic screening form. According to the data from the form, sixty-eight were males (69%) and thirty were female (31%). Sixty-three (64%) identified as White, fifteen percent as Asian (15%), eleven as Black or Hispanic (11%), and the remainder as "Other". Ninety-six hold a high school degree or higher (98%) and fifty-nine hold a bachelors degree or higher (60%). Fifty-two are under the age of 29 (53%), forty-two are between 30-49 (43%), and four are over the age of 50 (4%).

Participant Sample. From this sample, we selected 72 participants for interviews, attempting to stratify on age, race, gender, and education to achieve diversity. 20 of those selected attended their interview appointment (see Table 1 for an overview). Sixteen of the participants are male (80%), eleven are White (55%), seven are Asian (35%), and one participant identified as Hispanic (5%) and as Other (5%), respectively. All participants hold a high school degree (100%) or higher and ten hold a bachelor degree or higher (50%). Fourteen are under the age of 29 (70%), five are between 30-49 (25%), and one is over the age of 50 (5%).

Representativeness of Participant Pool and Sample. Both our sample of potential participants and our 20 participants are more male than the U.S. population (51% Male) [2], as White as the general population (62% in the U.S. population), more Asian (8% in the U.S.), more educated (87% hold a high school degree or higher and 30.3% hold a bachelors degree or higher), and younger (40% are under the age of 29, 26% are between 30-49, and 34% are over the age of 50 in the U.S. [1]).

VR Platform and Usage. Finally, nine of our ten users reported using an Oculus product, either the Rift or Gear, while the other used an HTC Vive. Of the nine Oculus users,

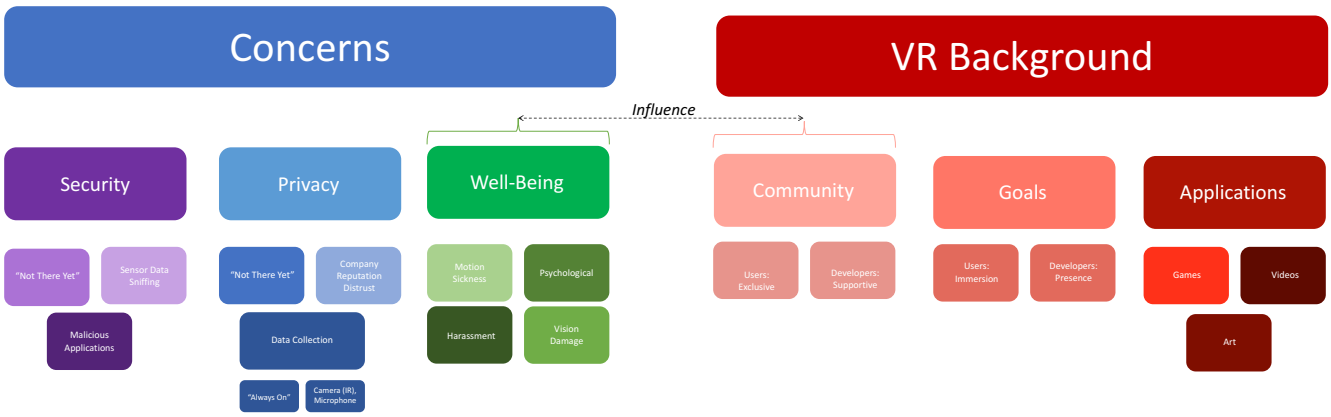


Figure 1: Diagram of the classes of concerns described by users as well as the components of their VR background that we analyze, and in some cases, find influences their concern perceptions.

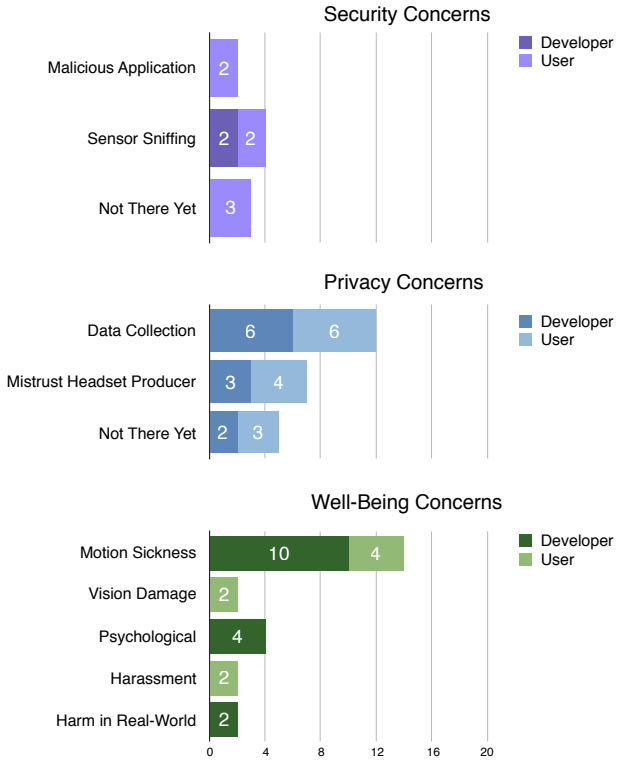


Figure 2: Counts of the number of developers and users who mentioned each type of concern during our interviews.

three also used other platforms, two a Google Cardboard and two the HTC Vive. Four users used their headsets for multiple applications, while the other six used their headset for multiple uses. In total, seven users used their headsets to watch videos, six used the headset to play games, and two used the headset for art experiences. Eight of the developers developed for Oculus Rift and Gear, three of whom also developed for HTC vive, the other two developers developed only for HTC Vive. Five reported developing games, three reported creating interactive art or videos, one reported creating a social application, one reported creating an educational tool, and the final developer reported creating a work-specific simulation.

ID	Sex	Age	Race	Educ.	Plat.	App.
U1	M	50-59	W	SC	C/O	V
U2	M	30-39	W	SC	O	V/G/S
U3	M	40-49	W	B.S.	O	V/G/A
U4	F	18-29	A	SC	H	O
U5	M	18-29	A	B.S.	O	V/G
U6	M	30-39	A	>B.S.	O	G
U7	F	30-39	A	B.S.	C/H/O	V/G/A
U8	M	18-29	W	SC	H/O	V
U9	F	18-29	W	B.S.	O	G
U10	M	18-29	A	B.S.	O	V
D1	M	18-29	W	SC	O	G
D2	M	18-29	A	H.S.	O	A
D3	M	18-29	W	SC	O	G
D4	F	18-29	H	SC	O	S
D5	M	18-29	O	B.S	H/O	G
D6	M	18-29	W	H.S.	H	G
D7	M	40-49	W	>B.S.	H/O	A/E
D8	M	18-29	A	SC	H	Other
D9	M	18-29	W	>B.S.	H/O	G
D10	M	18-29	W	B.S.	O	A

Table 1: Participant Demographics. Educ. is education level, Plat. is VR platform(s) used or developed for (O: Oculus Rift or Gear, H: HTC Vive, C: Google Cardboard), and App. is VR application types used or developed (V: video, G: games, A: art, S: social, E: education).

4.1.2 *Developer Interview Results*

Goals of VR development center around presence. The VR developers that were interviewed were creating a variety of experiences. Across these varied domains, the majority of developers (six) mentioned that their primary goal when developing was to facilitate and ensure a sense of "presence." For example, D9 says, "you have to focus all your design actions on making sure that you don't break the state of presence and you add to the immersive experience." D4 notes that well-being and security are closely intertwined with this goal: "motion sickness breaks presence, while presence enhances risks of psychological threat or someone screwing with people by getting into the virtual environment."

VR developer community is strong and enhances learning. When asked how they learned to develop for VR, five developers reported using online tutorials and three re-

ported signing up for a more structured online bootcamp or course. The other two developers, as well as six of the eight who also reported learning from only tutorials or bootcamps, also mentioned asking questions to other VR developers in various online communities. More broadly, four of the developers, without prompting, mentioned the strength of the VR community. For example, D10 says, "you could fit them all in a small room really, and it's really close, it's really tight knit. I actually became close friends with most of them even still to this day I consider them almost family in a way. And yeah, I have been developing for VR ever since [meeting other VR developers online]." Similarly, D7 describes an open, supportive community, "we are still in the phase in the industry where people are very open and willing to help each other and that's a huge blessing because we are still you know its still evolving and...instead of like hoarding knowledge, we need to sort of cross develop."

Concerns for user well-being encompass the physical and psychological. Developers' concerns for their users often focused on well-being. All of the developers raised concerns about motion sickness. For example, D6 says, "motion sickness isn't really a concern at all when developing for a game you are going to play on a computer screen. But when you're looking at VR, [motion sickness] is...a driving factor, you could say, in development."

Additionally two developers raised concerns about participants being unaware of danger in their real-world physical environment (e.g., not hearing fire alarm, bumping into objects as a result of game play). On this point, D1 says, "the biggest issue is probably letting people know that there needs to be a specific and safe environment to use VR. Because obviously you're not interacting with the rest of the world [while you're in VR]...[this is an] issue that I don't actually see very many people looking into. [For example,] say that you're in VR and a alarm fire goes off in the building, who is to say that you actually are going to hear that alarm...this disconnect from the actual world and the VR experience is a definite issue."

Four developers mentioned concerns with the psychological well-being of their users. D9 and D4 mention that harms (e.g., bullying or intentional scary moments) in VR may feel more realistic and thus may be more traumatizing. D9 explains, "VR is a very personal, intimate situation and when you wear a VR headset...you really believe it, it's really immersive. So if someone harms you in VR—either verbally or something else—you will also feel that after taking off the headset." Similarly, D4 says, "VR content is a lot more impactful...the feeling of like being scared in VR is much more real. Because everything does feel so real and so tactile, so you have to be extra careful with the content you are introducing to people." D8 and D5 express similar concerns, and also raise a connection between psychological swell-being and security—potential psychological harms that may come from a malicious entity being able to alter the VR experience. D8 says, "I think that it's on the developer to try and limit the user to being able to only experience what the developer was intending for them experience in the first place."

Developers mention privacy concerns about variety of issues. Six developers mention privacy concerns about VR, but none of them feel these concerns are relevant for their own products. Two mention concerns with the fact that the headsets are "always on" and users could be unaware of the data collection that is happening when they are not using their headset. Three others expressed concern about the ability of the headset to use camera sensors to detect users locations or to access the microphone in their space: "what somebody is doing while in VR is recordable and trackable on a different level" than on other digital platforms, which is something you "have to acknowledge," D8 notes.

Three developers mentioned privacy concerns specifically related to Facebook's ownership of Oculus and the developer's perception of Facebook's reputation around privacy issues. For example, D10 remarks on his perception of Facebook's attitude toward privacy, "they are not afraid to manipulate to see if you're happy or sad, they are not afraid to get caught, in the end, it's all about the money to them. It's not about these altruistic goals and that is definitely one of my biggest concerns hands down. That's why you know, Facebook acquired Oculus, so they could get a monopoly over the next form of advertising and control media and connecting people." D7 expresses a similar sentiment: "I think Facebook is pouring money into VR because it is going to generate this kind of super personal data that will help create a biological map or biological key, of who their users are."

On the other hand, two developers felt that VR "was not there yet" to worry about privacy. D4 likens VR to the early days of the Internet, "remember the beginning of the Internet and chat rooms, [in VR] potential issues haven't been addressed yet because it hasn't happened yet." The final two developers did not explicitly comment on privacy, despite being prompted.

Developers suggest permission requests to mitigate privacy concerns, yet no such capability exists for most headsets. Four developers suggest that using permission requests could help mitigate privacy issues for end users. For example, D8 recommends that VR should do something "identical to current privacy methodologies in terms of your requesting permission from the end user ahead of time." However, no desktop VR applications include any such permission requests (the Samsung Gear VR which runs off a Samsung phone does include permission requests, although it is unclear from the documentation whether there are permission requests made for e.g., camera sensors on the VR headset rather than phone sensors). D9 also recommends adding permission requests within the VR environment, but notes that this may be difficult to design because there is no single view point (e.g., screen) in VR: "if you want to [request] some information from the player you cannot simply display it on the screen because it is not there."

Finally, five developers recommend using privacy policies rather than permissions to help users make informed privacy and data collection choices. However, as summarized in Section 4.2 we find that, currently, few VR applications offer privacy policies that discuss VR data collection.

Little mention of security. Overall, when discussing potential concerns about VR, the developers we interviewed spoke the least about security. Two developers mentioned security concerns for health applications. For example, D6

says they would be concerned about security for applications used for "medical or for education [purposes]." For those applications, he says, "the issues with hacking are more serious. I think [that is where] protecting data [would be] important. But you know, there has got to be some serious push for that or else there would be no incentives...to do that right."

Two other developers mention security, but they reference passing off security responsibilities to others. For example, D5 explains that they use Unity and Google cloud storage to store data collected from the user. When asked about security they explain that they do so in part because, "it means that we don't have to deal with securing information ourselves. It makes it their problem and not ours."

Developers appear to take concerns about users' privacy and well-being on themselves. While these two developers passed off security responsibility to the storage services, it is interesting to note that no developers mentioned "passing-the-buck" for well-being or privacy. For example, while the OS would typically be key for managing permission requests and ensuring that information was shared only when it should be, no developers mentioned the responsibility of Windows- or Android-system developers to mitigate vulnerabilities and enforce permissions. (It is possible that the four developers who mentioned permissions meant to imply this.) More generally developers appeared to take responsibility for end-user privacy and well-being onto themselves, never mentioning that Oculus, HTC Vive, Windows, or Android could make improvements to address such issues. "it's gonna be something that developers have to...keep an eye on and implement" (D8).

Marked disconnect between developers' general security and privacy concerns and concerns about their own products. However, despite feelings of responsibility, there seems to be marked disconnects between developer's privacy- and security-related concerns for VR users in general and the privacy and security risks they see in their own products. While most of the developers who mention well-being concerns also mention working to mitigate these concerns for their own projects, the majority of those who mention privacy and security risks (5/6 for privacy and 2/2 for security) do not see privacy and security risks with their own products. For example, even D9, who raised security concerns and is working on an application that infers users health conditions via sensor data and then provides VR-based treatments says, "yeah I actually [can]not think of a privacy or security problem...[with my product] maybe it's an issue in the future."

Developers express desire for standards and ethical guidance. Finally, and perhaps relatedly, D5 notes that no one in the VR development community "is experienced" or is "an advisor" about ethics and privacy and security issues: "just the fact of the matter is there are no VR power users. You know I can count on the number of fingers the number of experienced 'devs' I've actually met." This lack of guidance, he says, makes it hard to "know where the right line is." Five other developers expressed similar sentiments, with D8 explaining "there's a quite a big list of unknowns right now in terms of what's best etiquette for a user and what's gonna keep them the most comfortable and satisfied in the experience. That has already been hashed out for web development over the last couple of decades [but not in VR]...[the VR] industry needs to start using standards."

Thus, D10 suggests that a "mantra" or code of ethics is needed, and suggests that the big companies are not going to step in, so an emphasis on ethics will need to come from developers themselves. He explains, "I would encourage developers to be transparent and to just not talk down to customers, don't treat them as numbers. Don't do onto others what you wouldn't want onto you. I'd like to have a mantra like that. And just because Facebook does something different doesn't mean I or anybody else [in the community] has to do that." Thus, we hypothesize that the disconnect between developer's general concerns for VR users and concerns about their own products may, in part, arise from inconsistent or ill-defined guidance about what should be a concern and what needs to be addressed in development. As explored more closely in Section 4.3 we take a first step toward helping the VR developer community define their desired code of ethics via a co-design study, resulting in the code of ethics shown in Figure 7.

4.1.3 User Interview Results

Immersiveness and, to a lesser extent addictiveness, are key user desires. We find that developer and user goals seem to be in alignment: the developers we spoke with focused their development around achieving "presence" and, similarly, we find that most users (7/10) sought out VR for the "immersiveness of the experience." As U8 explains, "I think it's really just about being immersed in a different type of world...As opposed to a TV where I can constantly be distracted. When I'm in VR...100 percent of my attention is dedicated to that because I can't text or I can't just multitask." Two users also mentioned that they *wanted* VR to be addictive: "VR needs that addicting label...those features that keep people going back again and again and again" (U4).

Majority of users learn about VR online. When asked how they learned about VR and selected the VR platform they use, users mentioned three primary information sources: friends and family (two users), the Internet (seven users), and school (one user). Of those who mentioned learning about VR from the Internet, three specifically mentioned learning about VR from Reddit: "Reddit is awesome for anything" U1 says. As U6 explains, one of the ways he learned about VR is by being a "group reddit with some friends and stuff". Further, after learning about VR, three users, including two of whom did *not* learn about VR from Reddit, reported relying on Reddit reviews to select their headset: "you read a 100 posts on something you're gonna get a good gauge on whether a product is good bad or otherwise" (U1).

Users' concerns about well-being are focused on the physical. Four users expressed concern about motion sickness in VR. However, their concerns, are more muted than developers were. U2 explains, "it happens to some people and doesn't happen to some others...it's basically an individual kind of thing so I just had an awareness...[it was] not so much a problem to be weighed." Two users also expressed a different type of physical concern, not considered by developers: vision deterioration from VR use.

Only one user—U2 who also brought up "awareness" of motion sickness—brings up concerns around psychological harms. He worries about other users who "aren't mentally

as strong," elaborating, "some people don't have the mind to handle things...I'm sure if you put a soldier into VR and play the wrong experience like Call of Duty or Battlefield or something like that. That could trigger some sort of... flashback or bipolar moment...really, what VR is trying to do here is duplicate reality where it tricks your mind into feeling like you are somewhere else. Some people might not be ready for something like that, some people might not be mentally developed enough to take something like that and not be messed up over it, you know?"

Finally, two other users bringing up a different type of well-being concern: cyberbullying / harassment. U8 expresses concern about harassment in the future, "For me, VR has just been pretty much stand alone. I haven't interacted with others in VR...[interacting with others] is, you know, a big concern. The type of people who are online: spouting racism, sexism. I mean if they have ability to [use] VR they're probably going to...know it will [become] like any message board."

More users than developers raised security concerns. Seven users raised concerns about security: four raised current concerns while the other three raised concerns about the future. U1 and U5 expressed concerns about the security of applications the experience stores. U1 says, "as soon as I moved over to the Gear [4], I didn't have as much concern as with the you know the old Cardboard glasses [5] where third parties could produce content that I could see. I'm aware of the concerns with vulnerabilities in those applications. I'm much more comfortable you know going through the Oculus store for the Gear [because] they do all the vetting and stuff up front." U6 and U10 raise concerns about malicious attackers modifying their virtual experience or gaining access to headset sensors. U10 believes that "someone could hack into your systems network...take control of your centers and using his camera to spy on you", but is "not really concerned about that". Similar to U10, U6 acknowledges that "there are different hacks you can do to change the game to have someone password or whatever".

U2, U4, and U7, on the other hand, are not concerned about security now, but would be concerned in the future as the VR industry expands. U4 says, "if VR gets the chance that it needs...that's when you're going to get to...worrying about hackers altering your experience. What's going to be crazy is at that point...[is] just like your buddy can pick up your phone and post on your Facebook, and everybody thinks it's you...someone can put on a VR head unit and go into a virtual world assuming your identity. I think that identity theft, if [VR] becomes mainstream, will become rampant." More generally, U7 explains, "I'm sure someone will figure out a way to exploit what we do. For now, everything is still new...we still haven't even figured out typing in VR. Like I feel like someone needs to invent technology [to monetize VR]...when people actually start making money in VR," that is when she thinks issues will arise.

Users worry most about microphone and infrared camera data collection. Six users expressed concern about privacy related to data collection. All six focused on microphones or infrared sensors in the headsets collecting data because these sensors are "always on, which I find is weird" (U6). U5 says, "the Rift actually has a microphone in it...[so I realized] oh crap people can hear me...I've [also] seen somebody who posted a picture of what the sensors actually picked up and it was a pretty clear view of the room and what not" (see Figure 3 for an example of an infrared image captured by the sensors on an Oculus Rift).

Figure 3: Image of Oculus Rift user's real-world environment captured by the infrared sensors on the headset [3].

Two users mentioned knowing that their headset collected this type of data about them, but said there was no reason to be worried unless "you were up to no good" (U7). For example, U2 explains, "if you're worried about something, you're up to something you shouldn't be doing. As far as what these things are going to collect, yeah you know...they could be collecting something...[but unless] you're doing something bad...what could they be collecting?"

Similar to security, three users felt that they would have more concerns about privacy in the future, but VR was not there yet. U8 explains, "I don't think there's probably anything. Because I'm just playing you know these little games...I think [privacy's] going to be a big concern of mine going forward especially when you know VR is more mainstream and more affordable."

Users raise privacy issues around headset producer reputation. Just as three developers raised concerns about privacy in the Oculus products due to the reputation of Facebook's approach toward privacy for their other services, four users raise similar concerns. U3 explains that these concerns about reputation are, "one of the reasons that I didn't install the Facebook app within virtual reality...it can read and write your contacts, it can call phones, it can send data to whoever whenever without you knowing." Similarly, U5 worries based on what he's heard in the news about Facebook, "considering that Oculus Rift is owned by Facebook, I [am] concerned...you know Facebook has been in the news recently about just how much information they pick up based on your habit, posting activities and other things like that."

Users vary in their comparative perception of privacy risk in VR. Overall, four users felt they were at more privacy risk on VR than on other platforms, four felt that

[4]The Samsung Gear is a headset produced by Oculus, which is owned by Facebook.
[5]U1 is referring to the Google Cardboard headset.

VR exposed them to the same level of risk as any other platform, and two felt that less data was collected about them on VR than elsewhere. U6 explains that he feels VR is the same as anything else because, "I've reached a point where I guess it's pessimism. Where I realize you know there's all these data breaches and hacks, you know, all of our information is out there so that after I got over that concern you know I just learned not to stress too much about it...So, I kind of took a pessimistic view towards privacy that way and I realize hey, they already have this information."

Users perceive the VR community as exclusive and, consequently, safe. Interestingly, four participants, unprompted, describe the community of other users on VR. They describe their community of peers as an exclusive one, which requires money and technical savvy to get in. For example, U4 says, there's a "high entry barrier to even get started in VR. Usually it's pretty high. You know people with disposable income and who are you know tech oriented. It's not just you know [anyone] typing on a keyboard."

Similarly, U2 describes the typical user he meets in VR as "somebody who has a lot of money and has a premium setup you know...I mean you are talking people with 4 plus sensors." This sense of exclusivity makes these four users feel safe, especially from well-being concerns around harassment. For example, U4 continues her above comment to explain that she will be more concerned about virtual crimes and bullying once VR becomes more accessible to the "general public." Similarly, U2 continues, "people in virtual reality are a lot more open, a lot nicer, they're a lot more accepting. You know, online, some people can be really rude, some people can be helpful, some people can be just annoying. I found that in VR you kind of bring back that element where you feel like you are looking at somebody in the face...The way that the market is right now, there is a specific group of people that are using these devices. So, it makes for interesting conversation. Usually the people you would meet online are not on Reddit. But, if I play with you on big screen [e.g., VR] most likely you would be on Reddit because there's a certain type of crowd that's really into this, you know?"

Some users evangelize VR, even buying headsets for others. Three of the users with whom we spoke specifically mentioned evangelizing VR to others. U6 says, "Oh I've already recommended to every person that came over to my house I've already brought my rig up to my parents to let them just play with it...I would recommend it to anybody." U2 even bought multiple headsets—and gave a headset to a friend—so that he could use VR with others and so that they could "experience the magic." Part of his motivation for doing so is social, he says, "one thing I noticed about virtual reality that kind of sucks is it can be a very solo, anti-social experience if you think about it...what you end up having is one person with glasses saying oh wow wow and everybody else is sitting there scratching their head like okay, hopefully I can try that in a few minutes. [I] found that the most you can get from these things will be when you actually link up a couple units. The social experience makes the entire thing a completely different game changer. When you are doing it with a couple other people, the social aspect completely turns VR into a totally different animal."

Two more users mention more tempered evangelizing, saying, "Like I think everyone should try it. I don't think everyone should necessarily buy it" (U7) and raising concerns around making recommendations too broadly because VR is so expensive. Finally, two users mention explicitly not recommending VR to others. U1 explains, " I'm certainly not the evangelical type to say oh you have to like it...I let them know it's out there and what's available and what the future holds" but, he says, some people get sick or don't have the right depth perception to make it right for them.

4.2 VR Privacy Policies

Overall, we find that 82% (74) of the Oculus experiences and 30% (15) of HTC Vive applications have a privacy policy posted on the page from which users can download the experience. [6] Of these privacy policies, 19% (14 of 74) of the Oculus policies mentioned VR or VR-specific data collection; 33% (5 of 15) of the HTC Vive policies did the same.

Some policies that did mention VR or VR-specific data provided vague descriptions (4 of 14 Oculus, none of the HTC Vive applications), refering the reader to the Unity or Oculus privacy policies or state that they will "collect the data you share with us" with no further detail. Seven of the 14 Oculus policies and 3 of the 5 Vive policies stated that they would only collect personal information such as the user's email address, billing code, phone number, and etc. Four of the Oculus policies explicitly mention inferring the user's movements, for example the *Virtual Desktop* privacy policy states, "Information about your physical movements and dimensions when you use a virtual reality headset." *Sprint Vector*'s policy spoke more broadly about biometrics and biofeedback, saying, "We may collect biometric and biofeedback information relating to your use of the Services, including information about your physical movements and dimensions when you use a virtual reality headset."

Finally, one Oculus policy and two of the five Vive policies warn that the experience captures audio or IR camera data. For example, *MetaTable Poker*'s policy explains that once you join the application, your microphone will be activated and everything you do and say will be transmitted to every player in room (and will be stored by the application).

4.3 Code of Ethics Co-Design

Our code of ethics document received 1053 views from our posts to 11 online communities. Of these viewers, we anticipate that 245 were able to potentially make an edit. The remaining viewers were on a mobile device, on which it is only possible to edit a Google doc if the app is installed and even then it takes multiple additional clicks to edit. Of these 245 people that we estimate could make an edit, 19 people made contributions—edits, comments, or additions of new sections—to the document. Figure 4 shows a screen-shot of the document about three-quarters of the way through contributions being added. Interestingly, contributions were made only asynchronously: no participants used the chat feature in GoogleDocs [7]. This may be because they did not want to communicate synchronously or because the chat was difficult to locate.

[6] See `https://www.oculus.com/experiences/rift/733640976736718/` for an example page from which an experience can be downloaded.

[7] `https://support.google.com/docs/answer/2494891?co=GENIE.Platform%3DDesktop&hl=en`

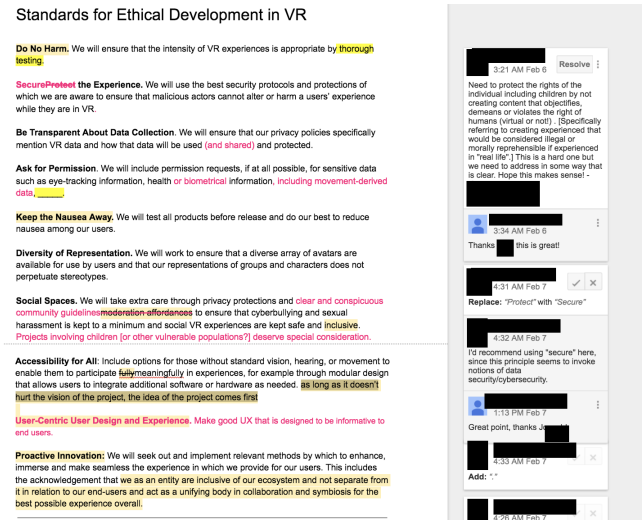


Figure 4: A screenshot of the code of ethics document about three-quarters of the way through the co-design process. Contributor names and researcher names have been blinded from the figure.

An additional seven people were "sharers"—people in the communities who indicated that they did not edit themselves, but were passing along the document to specific people to ask them to edit (or promote). Thus, we observe a phenomena similar to that observed in other editing scenarios such as Wikipedia editing: a large proportion (approx. 90% in our study) of lurkers in comparison with a small proportion of active editors [34].

Interestingly, while we offered a $2 incentive to those who made a contribution to the document, only one of the 19 contributors requested their incentive. We hypothesize that this may be due to the type of people choosing to contribute (those concerned about ethics may be more altruistic) or out of concern about anonymity (this hypothesis is less supported, as 10 of the 19 contributors revealed their names).

The initial code of ethics that we proposed had seven principles (the first seven shown in Figure 4). The developers contributing as part of our co-design modified the title and body for all but one of our proposed principles (Diversity of Representation was untouched). The contributors also added three additional principles: Accessibility for All, User-Centric User Design and Experience, and Proactive Innovation; all of which were subsequently edited or commented on by contributors other than the ones who proposed them.

The majority of contributions were edits (29 in total). Sometimes, edits were briefly explained—for example, as shown in Figure 4 one contributor changed "Protect the Experience" to "Secure the Experience" because they felt that "Secure" more clearly indicated a cybersecurity focus. The Social Spaces, Accessibility for All, and Ask Permission principles were the most edited, with six contributors editing Social Spaces and four contributors editing the other two, respectively. Each of the other sections had at least two edits. There were also 11 comments left on the document, with most sections receiving one or two comments.

Below, we present two case studies of the editing process: a case study of the process through which one of these new

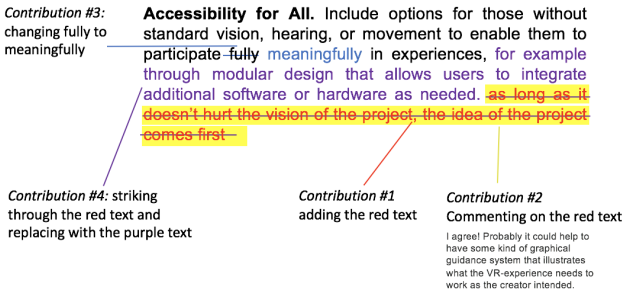


Figure 5: A diagram of the editing process for the Accessibility for All principle in the code of ethics document.

principles—Accessibility for All—was developed and a case study of the process of revision for one of our proposed principles: Social Spaces.

Case Study: Developing the "Accessibility for All" principle. One developer added the Accessibility for All section, after feeling that there was not enough emphasis on inclusivity in the existing code. She commented on the word inclusivity (originally in the Social Spaces principle), saying, "need to add [inclusivity] as a different heading and not under Social Spaces: "Accessibility for all", having options for those without standard vision, hearing, or movement. (If you don't add this in from the beginning, then we will be having to kludge that in afterwards, and it just don't work well.)" She then added an Accessibility for All section. Subsequently, four other contributors commented on or edited the section. We diagram the changes in Figure 5.

The first contributor added a sentence weakening the proposed section, suggesting that inclusivity should not come before the vision of the product. The second contribution was a comment following up on this edit, agreeing, and, as we interpret it, suggesting that people with disabilities could be told what extra hardware they would need to get the same experience—seemingly a compromise between the original contribution and the edit. The third contribution was an edit, changing meaningfully to fully. This contribution also appears to have been executed in response to the conversation about the added line from contribution #1. This third contribution was explained by the contributor as follows: "I'd amend this to "meaningfully" instead of fully. Substitution of faculty is only a substitution and not a full restoration. "meaningful" interaction that facilitates their involvement and acknowledges their particular needs is more appropriate - even if [special] hardware to interface as required without specifically tailoring the experience around their needs. This would be a better approach (I believe) and therefore address the need for maintaining the vision of said project without negating [inclusion] at any point." Finally, a fourth contribution was made, which synthesized the comments from the second and third contributions—the fourth contributor removed the red line added by contributor one and added a more moderate statement recommending modular design so that users with accessibility needs could add hardware (as suggested by contributor #2's comment) to obtain a similarly meaningful experience.

Case Study: Modifying the "Social Spaces" principle. Figure 6 summarizes the contributions made to the

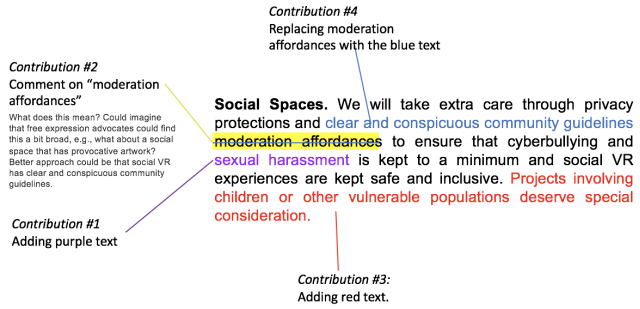
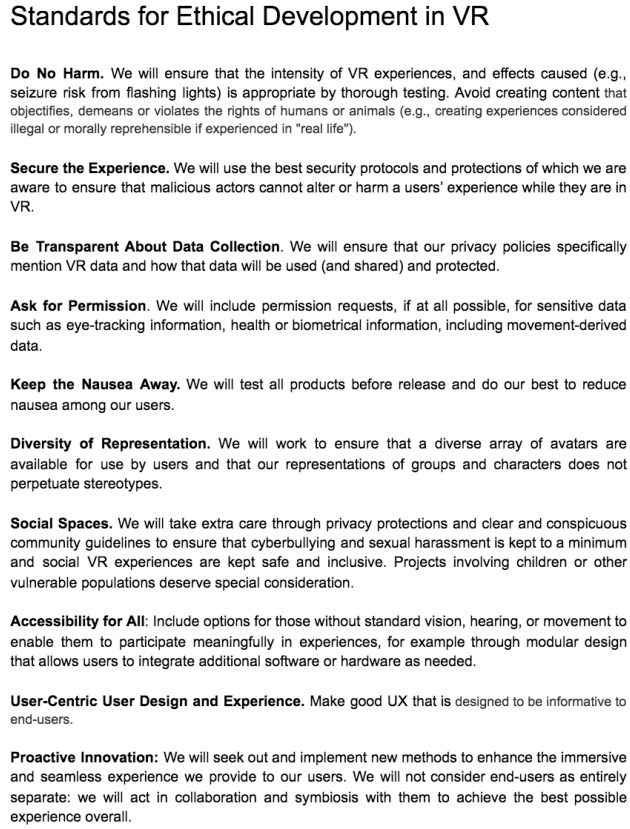


Figure 6: A diagram of the editing process for the Social Spaces principle in the code of ethics document.

"Social Spaces" principle, which we had proposed in the original code of ethics document. The first edit explicitly added sexual harassment to the types of negative experiences the principle would focus on preventing. The contributor who added this explained her contribution as follows: "As a female who has already experienced this kind of B.S. in the VR world, I think it's very important that this kind of unwanted behavior is spelled out to users and kept to a minimum by developers." Subsequently, the next contributor commented on the language "moderation affordances" suggesting that it might be better to post rules openly but not have moderators because moderation could inhibit free speech. Contribution #3 added text to encourage special consideration of children and other vulnerable populations. The second contributor then returned the next day to act on their comment about moderation, they made contribution #4: changing the moderation section of the text to reflect their prior comment.

In sum, these case studies illustrate the different ways in which developers interacted to collaboratively create the code of ethics. Some contributors engaged asynchronous back-and-forth with others to develop a certain section, even debating whether the other's contributions made sense. Some contributors explained their edits via comments while others simply edited with no explanation at all. Ethics were, at times, controversial—as exemplified in the Accessibility for All case study—but in all cases the contributors were able to reach a consensus. Overall, contributors appeared to exhibit respect for each other—even if debates became heated at times: "Wtf does that even mean?"—typically providing affirmation to each other and then working to incorporate other's comments or intentions into their future revisions.

After the 29 edits and 11 comments made by 19 contributors [8], the code of ethics shown in Figure 7 was produced.



Standards for Ethical Development in VR

Do No Harm. We will ensure that the intensity of VR experiences, and effects caused (e.g., seizure risk from flashing lights) is appropriate by thorough testing. Avoid creating content that objectifies, demeans or violates the rights of humans or animals (e.g., creating experiences considered illegal or morally reprehensible if experienced in "real life").

Secure the Experience. We will use the best security protocols and protections of which we are aware to ensure that malicious actors cannot alter or harm a users' experience while they are in VR.

Be Transparent About Data Collection. We will ensure that our privacy policies specifically mention VR data and how that data will be used (and shared) and protected.

Ask for Permission. We will include permission requests, if at all possible, for sensitive data such as eye-tracking information, health or biometrical information, including movement-derived data.

Keep the Nausea Away. We will test all products before release and do our best to reduce nausea among our users.

Diversity of Representation. We will work to ensure that a diverse array of avatars are available for use by users and that our representations of groups and characters does not perpetuate stereotypes.

Social Spaces. We will take extra care through privacy protections and clear and conspicuous community guidelines to ensure that cyberbullying and sexual harassment is kept to a minimum and social VR experiences are kept safe and inclusive. Projects involving children or other vulnerable populations deserve special consideration.

Accessibility for All: Include options for those without standard vision, hearing, or movement to enable them to participate meaningfully in experiences, for example through modular design that allows users to integrate additional software or hardware as needed.

User-Centric User Design and Experience. Make good UX that is designed to be informative to end-users.

Proactive Innovation: We will seek out and implement new methods to enhance the immersive and seamless experience we provide to our users. We will not consider end-users as entirely separate: we will act in collaboration and symbiosis with them to achieve the best possible experience overall.

Figure 7: The final VR developer code of ethics.

5. DISCUSSION & FUTURE DIRECTIONS

Below, we highlight takeaways and areas of future work.

Collaboration with Developer Communities May Improve Application Privacy and Security. In our code of ethics co-design study we found engagement levels typical of Wikipedia editing communities and observed that VR developers were able to effectively work together to reach consensus on a code of ethics. Our interview results suggest that VR developers rely on each other, through the small and supportive community they describe, to figure out how best to build applications for end-users, including how to secure applications, respect user privacy, and ensure well-being. VR developers do not appear to seek out this guidance from the companies creating the platforms, as some developers express distrust of the headset producers, with one developer saying, for example, "Don't do onto others what you wouldn't want onto you...just because Facebook does something...doesn't mean [I] have to do that."

The success of our co-design study and developers' sustained engagement with the document (100 views every three days, plus additional shares, since the study period ended) suggests that collaborative work with developers, such as future co-design work for additional standards and/or training of security or privacy peer advocates (such as those in workplaces [20])—who could provide guidance to their peers on how to design affordances for privacy and well-being or technical advice for avoiding code insecurities—may be an effective methods for improving applications for end-users.

While other prior work has similarly investigated how developers make ethical decisions in different domains [45, 44, 19], neither the work presented here nor this prior work has moved from inquiry to action: using collaboration and social influence with developers to drive privacy and security improvements. There is, however, support that such an approach may be useful, as social influence has been shown to be effective for promoting security behavior among

[8]Five days after the last activity on the document we accepted outstanding edits and made small editorial corrections for reading ease.

end-users [13]. Thus, future work may wish to investigate whether such strong communities exist for other types of development (e.g., IoT apps, certain types of mobile phone application development) and, if so, how to leverage collaborative interventions with these communities to solve developer-driven security and privacy issues raised by prior work [4, 51].

Users' Threat Model Includes Exclusivity of Community. Our results underscore a strong role of community not only for developers but also for users. Four of the users we interviewed described the VR community as small, exclusive, and consequently: safe. They mentioned that they would start to have concerns about security, privacy, or harassment later on but they were not currently concerned because the community was "nice" and the "people aren't like that."

While the close-knit nature of the user community makes users feel safer, such exclusivity has a downside: lack of diversity (as observed at a small scale in the demographic bias of the pool of potential participants recruited for our interview study). Lack of diversity among technology "innovators" is a known problem and exacerbates the digital divide [52, 21]: if no "innovators" from particular social groups are present, concerns these groups have may not be identified or addressed, applications of the technology that are of interest to these groups may not be developed, and these groups do not have an influencer to expand adoption of the technology in their community.

Further, the attitude expressed by some of the VR users in our study—that they did not want the "general population" to begin using VR—suggests that expanding the groups using VR may be difficult not just due to problems of access, but also due to exclusionary attitudes and narrow perceptions of who the users of VR are or should be (e.g., one user explained "the way that the market is right now, there is a specific group of people that are using these devices...Usually the people you would meet online are not on Reddit. But, if I play with you on big screen [e.g., VR] most likely you would be on Reddit because there's a certain type of crowd that's really into this, you know?").This desire for exclusivity among users contrasts with the emphasis that developers in our co-design study placed on Accessibility for All (accommodating those with disabilities) and Diversity of Representation (offering diverse avatars).

To increase the diversity of early adopters of VR, producers of VR headsets or technology activism organizations may wish to place VR booths or arcades in communities to enable access to those who cannot purchase a headset for their home or may consider providing headsets to Beta testers (e.g., "influencers") who sign up within communities with no adopters [23]. Future work may wish to explore the efficacy of such approaches and investigate the risks and experiences of populations who were not well represented in this study.

Looking Forward: Harassment, Security, and Policy. Overall, we find developers to be more focused on and concerned about well-being, including both motion sickness and psychological well-being (e.g., insuring that experiences are not too intense) than users, perhaps because developers are doing a good job at mitigating these issues. However, as new developers join it will be important to ensure that addressing these well-being related facets of VR risk remains a high priority, as emphasized by a recent news piece on one user's traumatic seizure in VR [9].

We find that one well-being risk not mentioned by developers is harassment. Only users mention any harassment concerns, suggesting that such concerns may be an emerging issue especially with increasing adoption of VR and increasing release of social applications.

Additionally, very few developers, and relatively few users, expressed security concerns – many explaining that VR did not have a big enough user base and was not monetized enough to be concerned. Given this attitude, it is likely that many early VR applications will have a number of security vulnerabilities and that vulnerabilities may increase with accelerating adoption. Raising developer awareness about potential problems early, which may require additional VR-focused research similar Roesner et al.'s work on AR threats [41] and can perhaps be achieved through approaches like those discussed above, may help stop problems before VR becomes a more enticing target for attackers.

Both users and developers did raise privacy concerns. Developers primarily suggested mitigating concerns around data collection (the majority of privacy concerns expressed by both groups) through "notice and choice": that is, the use of privacy policies. However, our findings show that VR privacy policies are currently lacking – either not posted or not mentioning VR data (e.g., what data they are collecting) – and prior work shows that privacy policies are hard for users to read and largely ineffective [30, 12, 37]. Further, as one developer in our study noted, desktop VR does not currently use permissions, in part because of the difficulty of presenting a permission screen in the virtual environment. Future work may wish to expand beyond exploring VR authentication [54, 18, 5, 6] to also consider permissions and data transparency solutions.

Finally, the application developers with whom we spoke felt that they needed to lead and take responsibility for addressing risks to end-users. This emphasis seemed largely to be due to concern with the reputation of the developers of the headsets, which was expressed by both users and developers. While it is important for application developers to be part of the ecosystem designed to keep users safe, future work may wish to explore policy and system-level guidelines, especially for privacy policies (GDPR legislation which explicitly requires companies to discuss the type of data they are collecting, its' uses and a justification for that use, and a way to opt out of many of the data collection types may be a step in the right direction) and medical and educational applications that touch on HIPPA- or FERPA-regulated data, such that the burden of protecting users does not fall only on application developers.

In sum, our initial results are encouraging: developers express significant concern about end-user risks and exhibited an interest in engaging in developing solutions in our co-design study. But, our results also underscore that issues around harassment and security may be coming, especially as many developers exhibit a disconnect between identifying general concerns for users and concerns with their own products and many users feel that they do not yet need to worry.

6. REFERENCES

[1] U.S. Census Bureau Age facts. https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ACS_16_5YR_S0101&prodType=table.

[2] U.S. Census Bureau QuickFacts. https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ACS_16_5YR_DP05&src=pt.

[3] What does the cv1 sensor/camera see?

[4] Y. Acar, S. Fahl, and M. L. Mazurek. You are not your developer, either: A research agenda for usable security and privacy research beyond end users. In *SecDev*. IEEE, 2016.

[5] M. Agarwal, M. Mehra, R. Pawar, and D. Shah. Secure authentication using dynamic virtual keyboard layout. In *ICWET*. ACM, 2011.

[6] F. A. Alsulaiman and A. El Saddik. A novel 3d graphical password schema. In *VECIMS*. IEEE, 2006.

[7] D. Bajde, M. Bruun, J. Sommer, and K. Waltorp. General public's privacy concerns regarding drone use in residential and public areas. 2017.

[8] V. Chang, P. Chundury, and M. Chetty. Spiders in the sky: User perceptions of drones, privacy, and security. In *CHI*.

[9] P. A. Clark. Someone had a seizure in vr and nobody knew what to do, 2018.

[10] R. A. Clothier, D. Greer, D. Greer, and A. Mehta. Risk perception and the public acceptance of drones. *Risk analysis*.

[11] S. Cobb and et al. Virtual reality-induced symptoms and effects (vrise). *Presence: teleoperators and virtual environments*, 1999.

[12] L. F. Cranor. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.*, 2012.

[13] S. Das, A. D. Kramer, L. A. Dabbish, and J. I. Hong. The role of social influence in security feature adoption. In *CSCW*. ACM, 2015.

[14] L. De Paolis and A. Mongelli. *Augmented and Virtual Reality*. AVR, 2015.

[15] T. Denning, Z. Dehlawi, and T. Kohno. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies. In *CHI*. ACM, 2014.

[16] J. Francis and et al. What is an adequate sample size? Operationalising data saturation for theory-based interview studies. *Psychology and Health*, 2010.

[17] R. S. Geiger and D. Ribes. Trace ethnography: Following coordination through documentary practices. In *HICSS*. IEEE, 2011.

[18] C. Goerge and et al. Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality. In *NDSS*, 2017.

[19] I. Hadar, T. Hasson, O. Ayalon, E. Toch, M. Birnhack, S. Sherman, and A. Balissa. Privacy by designers: software developers' privacy mindset. *Empirical Software Engineering*, 2017.

[20] J. M. Haney and W. G. Lutters. The work of cybersecurity advocates. In *CHI*. ACM, 2017.

[21] E. Hargittai. The digital divide and what to do about it. *New economy handbook*, 2003.

[22] 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 Symposium*, 2013.

[23] V. Kameswaran, L. Cameron, and T. R. Dillahunt. Support for social and cultural capital development in real-time ridesharing services. *CHI*, 2018.

[24] O. S. Kerr. Criminal law in virtual worlds. 2008.

[25] P. Klasnja, S. Consolvo, T. Choudhury, R. Beckwith, and J. Hightower. Exploring privacy concerns about personal sensing. *Pervasive Computing*, 2009.

[26] K. Lebeck, T. Kohno, and F. Roesner. How to safely augment reality: Challenges and directions. In *HotMobile*. ACM, 2016.

[27] L. N. Lee, S. Egelman, J. H. Lee, and D. A. Wagner. Risk perceptions for wearable devices. *CoRR*, 2015.

[28] M. Lombard, J. Snyder-Duch, and C. C. Bracken. Content analysis in mass communication: Assessment and reporting of intercoder reliability. *Human communication research*, 2002.

[29] G. Maganis and et al. Sensor tricorder. In *ACM MCSA*.

[30] A. M. McDonald and L. F. Cranor. The cost of reading privacy policies. *ISJLP*, 2008.

[31] T. Merel. The reality of vr/ar growth. https://techcrunch.com/2017/01/11/the-reality-of-vrar-growth/, 2017.

[32] V. Motti and K. Caine. *Users' Privacy Concerns About Wearables*. 2015.

[33] J. W. Nelson. A virtual property solution: How privacy law can protect the citizens of virtual worlds. *Okla. City UL Rev.*, 2011.

[34] B. Nonnecke and J. Preece. Lurker demographics: Counting the silent.

[35] F. O'Brolcháin and et al. The convergence of virtual reality and social networks: threats to privacy and autonomy. *Science and engineering ethics*, 2016.

[36] A. N. Oppenheim. *Questionnaire design, interviewing and attitude measurement*. 2000.

[37] I. Pollach. What's wrong with online privacy policies? *Communications of the ACM*, 2007.

[38] E. Rader and J. Slaker. The importance of visibility for folk theories of sensor data. In *USENIX SOUPS*, 2017.

[39] A. Raij, A. Ghosh, S. Kumar, and M. Srivastava. Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. In *CHI*. ACM, 2011.

[40] A. Rizzo, J. Pair, P. J. McNerney, E. Eastlund, B. Manson, J. Gratch, R. Hill, B. Swartout, et al. Development of a vr therapy application for iraq war military personnel with ptsd. *Studies in health technology and informatics*, 2005.

[41] F. Roesner, T. Kohno, and D. Molnar. Security and privacy for augmented reality systems. *Communications of the ACM*, 2014.

[42] J. Roettgers. Study predicts fewer than 10 million monthly u.s. vr headset users this year, 17 million by 2019. http://variety.com/2017/digital/news/vr-headset-data-mau-2017-2019-1202440211/,

2017.
[43] E. M. Rogers. *Diffusion of innovations*. Simon and Schuster, 2010.
[44] K. Shilton. Four billion little brothers?: Privacy, mobile phones, and ubiquitous data collection. *Communications of the ACM*, 2009.
[45] K. Shilton. Values levers: Building ethics into design. *Science, Technology, & Human Values*, 2013.
[46] The Franklin Institute. What's the difference between ar, vr, and mr?
[47] Virtual Reality Society. The history of virtual reality.
[48] Y. Wang, H. Xia, Y. Yao, and Y. Huang. Flying eyes and hidden controllers: A qualitative study of people's privacy perceptions of civilian drones in the us. *PoPETS*, 2016.
[49] I. Warren and D. Palmer. *Crime risks of three-dimensional virtual environments*. PhD thesis, Australian Institute of Criminology, 2010.
[50] D. Wen, X. Zhang, and J. Lei. Consumers' perceived attitudes to wearable devices in health monitoring in china: A survey study. *Computer Methods and Programs in Biomedicine*, 2017.
[51] P. Wijesekera, A. Razaghpanah, J. Reardon, I. Reyes, N. Vallina-Rodriguez, S. Egelman, and C. Kreibich. âĂIJis our children's apps learning?âĂİ automatically detecting coppa violations.
[52] S. Willis and B. Tranter. Beyond the 'digital divide' internet diffusion and inequality in australia. *Journal of sociology*, 2006.
[53] R. Yao and et al. Oculus vr best practices guide. *Oculus VR*, 2014.
[54] Z. Yu, H. Liang, C. Fleming, and K. Man. An exploration of usable authentication mechanisms for virtual reality systems. In *IEEE APCCAS*.

APPENDIX

A. ADVERTISING

A.1 Groups in Which We Advertised

We advertised in the following groups to recruit our interview participants.

- Reddit
  1. R/GearVR: Forum for users of Oculus Gear headset.
     `www.reddit.com/r/gearvr`
  2. R/googlecardboard: Forum for users of Google-Cardboard VR headset.
     `www.reddit.com/r/googlecardboard`
  3. R/oculus: Forum for users of Oculus to discuss VR.
     `https:www.reddit.com/r/oculus`
  4. R/RiftForSale: Forum for people to buy or sell VR tech.
     `www.reddit.com/r/RiftForSale`
  5. R/steamVR: Forum for VR users to discuss STEAM VR games.
     `www.reddit.com/r/steamvr`
- Facebook
  6. Virtual reality group: Facebook group for users and developers of VR to discuss VR.
     `www.facebook.com/groups/virtualrealitys/?fref=ts`
  7. Oculus Rift group: For Oculus and VR users and developers to discuss VR platforms that focus on the Oculus Rift.
     `www.facebook.com/groups/OculusRift/`
  8. Women in VR/AR group: For women developing in VR and AR to discuss opportunities and etc.
     `www.facebook.com/groups/womeninvr/`
  9. Oculus Rift Users Au group: Users of VR to discuss topics about VR that pertain to the Oculus Rift.
     `www.facebook.com/groups/277312492704516/`
  10. Google Cardboard: Users of Google Cardboard.
      `www.facebook.com/groups/1568155100117690/`
  11. Google Cardboard Developers: Developers of Google Cardboard.
      `www.facebook.com/groups/cardboarddev`
  12. Virtual Reality Gear: Oculus Rift, HTC Vive, Gear VR, Microsoft MR, PS VR, Oculus Go, Virtual Reality. Oculus Santa Cruz, Vive Focus, Occipital Bridge, Daydream, ODG R8, ODG R9, Pimax 8K, and OSVR users and developers.
      `www.facebook.com/groups/gearvr/about/`
  13. Daydream and ARCore: For professional enthusiasts, UX Designers, Programmers, Unity & Unreal Engine Developers, Artists, and other VR professionals who use Google Products like ARcore and Daydream.
      `www.facebook.com/groups/daydreamvirtualreality/`
  14. AR & VR Developers: Everything developers need to know about: augmented and Virtual reality (VR), Mixed reality, VR/AR apps & games development, and Hardware
      `www.facebook.com/groups/ARVRMR/about/`
  15. Two institution-related groups omitted for blinding.
- Forums
  17. Oculus General Forum: The Offical Oculus website forum.
      `forums.oculusvr.com/community/categories/general`

We advertised our co-design study to groups that were explicitly developer focused or from which we recruited the most developers, groups 1-5, 6, 7, 8, 13, 14, 15.

A.2 Advertising Text

A.2.1 Interview Study

The following advertising text was posted in the 17 online communities to recruit participants to complete our screening questionnaire for the interview study.

> Join an Exciting Study on Virtual Reality
>
> Are you 18 or over the age of 18? Do you use VR systems or applications?
>
> If you answered YES to these questions, you may be eligible to participate in a virtual reality research study.
>
> We want to talk to you about your experience using a VR system. We want your input for a 20

minute interview! Interviews will be conducted over the phone or through Skype. Participants will be compensated with a $15 Amazon gift card.

A.2.2 Code of Ethics Co-Design Study

The following advertising text was posted in nine VR developer online communities to recruit developers to contribute to the design of a VR developer code of ethics.

> tl;dr edit this document: [url] to help create a collaborative VR developer code of ethics. Email [address] to get a $2 amazon gift card for helping out!
>
> Long explanation: You might remember us from a post a little while back. We are a team of researchers studying development, security, and privacy in VR. As part of this project we interviewed developers from the VR community (thank you for participating!) about their experiences developing, what they see as the safety, security, and privacy concerns in VR, and etc. We also interviewed VR users about their use of VR and their concerns.
>
> One of the key points raised by developers was that there is no standardized "code of ethics" or "instruction sheet" for what to do with user data, how to notify users of data use, and how to practice ethical VR development.
>
> We would like to invite you to come together as a community (the strength and openness of the VR development community was also a common theme mentioned in the research), with our support, to develop a set of standards for ethical development in VR.
>
> Every contributor to the code of ethics will receive a $2 amazon gift card as a "thank you" from our team. We will host the code of ethics on a public website once it is finished and credit you (if desired) for your hard work, as well as publish the code in the research paper we are preparing.

B. INTERVIEW PROTOCOL

The following protocols were used during the 20 minute semi-structured interview conducted via phone, Skype, or Google hangouts.

B.1 Developers

Introduction

Hello. My name is [INSERT NAME] and this is [INTRODUCE OTHER PERSON]. Today we will be conducting a study on virtual reality.

Today we are going to chat about your experiences with virtual reality. I expect that our conversation will take approximately 30 minutes.

Motivations

I'd like to start our conversation with a discussion of what made you want to develop applications or systems for virtual reality.

1. How did you get into developing for VR?
2. Why did you choose VR?

Skill Acquisition

Next I would like to talk about how you learned the skills for your VR development.

1. How did you learn to develop on VR?
2. What resources or tools did you use to learn VR development?
3. Which ones?
4. Did you talk to anyone to learn to work with VR?
5. What do you feel is different about developing for VR?
6. Do you have any different concerns when you are developing?

Concerns

1. What are you currently developing or what have you developed for VR?
2. Why did you decide to develop this product?
3. What does your product do?
4. Do you foresee any barriers [if product already released: are there any barriers you feel are currently] preventing your product from reaching the market saturation you want to achieve?
5. How do you plan to address these barriers?
6. Do you forsee any privacy and security concerns with your product or VR in general?
7. For each concern: why?

Data Collection

1. What user data does your product collect?
2. For each data type: What are you planning to do with this data?
3. If no collection reported: What type of data could you collect? What might it be used for?
4. Do you think that users will be [/would be] concerned about this data being collected?
5. Why/why not?

Recommendations

1. (if sensible based on prior answers) How would you educate other developers on privacy and security risks for VR?
2. What do you wish you had known?
3. What materials would you like to have had access to?
4. In general, what advice would you give to someone wanting to develop with VR?
5. What information or resources would you point to for someone wanting to learn about developing VR?

B.2 Users

Introduction

Hello. My name is [INSERT NAME] and this is [INTRODUCE OTHER PERSON]. Today we will be conducting a study on virtual reality.

Today we are going to chat about your experiences with virtual reality. I expect that our conversation will take approximately 20 minutes.

Motivations

I would like to begin with a few questions about your current use of VR.

1. How long have you been using VR?
2. How did you learn about VR?
3. What made you decide to buy/use a VR headset?
4. Ask why for each thing they mention?
5. Why did you choose your particular VR software over others?
6. Where did you go to find out information about the systems?
7. What do you usually do with VR?
8. What do you see as the benefits of virtual reality?
9. What were your goals when you started using these systems?

Concerns

1. When you were making your purchase, did you have any concerns?
2. Why/why not?
3. What about with your specific headset?
4. Did you worry about privacy at all when you were deciding whether to purchase the system?
5. Could you tell me a bit more about your concerns with <each item>
6. Do you still have these concerns?
7. Do you do anything to try to prevent this?
8. How about security, any concerns there?
9. Could you tell me a bit more about your concerns with <each item>
10. Do you still have these concerns?
11. Do you do anything to try to prevent this?

Data Collection

1. Do you think your virtual reality system collect information about you?
2. What do you think it collects?
3. How do you think this information is used?
4. Are you concerned by this?
5. Would you say you feel differently about this than about data that gets collected by your other devices? Why?

Recommendations

1. How likely is it that you could recommend VR to a friend or colleague?
2. What concerns would you share or discuss?