Understanding Parents' Perceptions and Practices
Toward Children's Security and Privacy in Virtual Reality

Jiaxun Cao
Duke University
jessie.cao@duke.edu

Abhinaya S.B.
North Carolina State University
asrivid@ncsu.edu

Anupam Das
North Carolina State University
anupam.das@ncsu.edu

Pardis Emami-Naeini
Duke University
pardis@cs.duke.edu

Abstract—Recent years have seen a sharp increase in the number of underage users in virtual reality (VR), where security and privacy (S&P) risks such as data surveillance and self-disclosure in social interaction have been increasingly prominent. Prior work shows children largely rely on parents to mitigate S&P risks in their technology use. Therefore, understanding parents' S&P knowledge, perceptions, and practices is critical for identifying the gaps for parents, technology designers, and policymakers to enhance children's S&P. While such empirical knowledge is substantial in other consumer technologies, it remains largely unknown in the context of VR. To address the gap, we conducted in-depth semi-structured interviews with 20 parents of children under the age of 18 who use VR at home. Our findings highlight parents generally lack S&P awareness due to the perception that VR is still in its infancy. To protect their children's interactions with VR, parents currently primarily rely on active strategies such as verbal education about S&P. Passive strategies such as using parental controls in VR are not commonly used among our interviewees, mainly due to their perceived technical constraints. Parents also highlight that a multi-stakeholder ecosystem must be established towards more S&P support for children in VR. Based on the findings, we propose actionable S&P recommendations for critical stakeholders, including parents, educators, VR companies, and governments.

1. Introduction

The growing popularity of consumer-facing virtual reality (VR) in recent years has attracted a significant number of users [1], [2], including children under the age of 18 [3], [4], [5]. While immersive and realistic experiences provide great user engagement, more risks have been emerging in VR, including safety, well-being, security, and privacy (S&P) issues [6]. Specifically, VR devices collect a variety of sensitive data [7], including eye- and motion-tracking data that are indispensable for immersion yet pose risks of data surveillance [7], [8], [9]. Worse yet, S&P experts have been warning people of the scarce, unspecific, and under-enforced privacy policies in VR [7], [10], [11], [12].

Furthermore, users including children have flooded social VR applications (e.g., Horizon Worlds, Rec Room, and VRChat) [3], [4], [5], raising S&P concerns. In internet-enabled social VR applications, besides data surveillance, users also face S&P risks in social interaction, including self-disclosure [13]. Prior work has suggested that social VR users easily disclose a wide range of personal information to strangers, including emotions, life experiences, voices, and even real-life appearances [13].

In particular, these S&P risks in VR can be heightened for children, especially considering the largely age-mixed environment in VR [3], [4], [5]. Prior work has investigated common risks that children encounter in social VR, including virtual harassment, cyberbullying, and inappropriate content from both peers and adults [3], [4], [5]. However, one important limitation of the existing literature is that while general safety risks have been widely documented, S&P-specific risks in VR have been largely overlooked.

In mitigating S&P risks in technologies, children heavily rely on parents' S&P knowledge and decision-making [14], [15], [16]. Researchers have suggested that children trust parents' S&P rules and tend to seek help from parents when risks emerge [16]. Moreover, parents' S&P perceptions might influence how children conceptualize and perceive S&P [17], [18], [19]. In addition, parents also adopt a variety of strategies when mediating children's technology use, including passive strategies (e.g., parental controls) and active strategies (e.g., verbal education) [16], [20], [21], [22]. When adopting different strategies, parents might also face different challenges in mitigating risks, such as low familiarity with technology [23], [24]. Therefore, understanding parents' S&P perceptions and practices is crucial for researchers and other important stakeholders to support parents' risk mitigation strategies. While such knowledge regarding other technologies (e.g., smartphones [25], [26], Internet-enabled applications [16], [27]) has been fully investigated, it remains unknown in the context of VR. Hence, this work aims to answer three research questions (RQs):

- **RQ1**: What are parents' perceptions of children's S&P in VR?
- **RQ2**: What are parents' risk mitigation strategies for their children's S&P in VR?
- **RQ3**: What are parents' expectations toward perceived critical stakeholders and future S&P-enhancing features in VR?

To address the RQs, we recruited 20 parents whose

children use VR applications at home. We conducted semi-structured interviews to surface their perceptions of S&P risks for children in VR. We then asked parents how they addressed their concerns, if at all. Last, we asked them to propose critical stakeholders and desired features in protecting children's S&P in VR.

Our qualitative analysis reveals three main points. (1) First, although parents typically do not have immediate S&P concerns for their own children, they do express concerns for underage VR users in general and anticipate more pressing risks for their own children in the future. (2) Second, parents adopt a limited range of strategies when mediating children's VR usage. Specifically, parents rely on active strategies such as verbal education more than passive ones, including parental controls. While acknowledging the potential effectiveness of passive strategies, parents face significant technical constraints in practice. (3) Finally, parents agree on four critical stakeholders – parents, educators, VR companies, and governments. They also propose a series of potential features to enhance existing S&P controls in VR, with a few reservations about using them.

Based on parents' rich insights, we provide actionable recommendations for the critical stakeholders. In brief, we urge parents, educators, and governments to enhance their nuanced understanding of VR technologies, as their current S&P practices are overgeneralized across all digital devices. We also encourage parents and educators to set physical references when educating children about S&P risks in VR. In addition, we propose that VR companies should involve engagement, granularity, and modality-specific considerations in their designs of S&P controls. Finally, we call for VR companies to enhance their user guidance on S&P risks in VR, along with regulators' enhanced supervision over VR companies' S&P practices.

2. Related Work

S&P risks in VR. VR technologies collect a vast amount of sensitive data that has been categorized by Dick [7] into four types – (1) observable data that generate users' virtual presence, e.g., avatars and real-time in-world interactions [28], [29]; (2) observed data that enhance immersive experiences, e.g., motion/eye-tracking [8], [9], [29], [30], [31]; (3) computed data that improve user services, e.g., user profiles for advertisements; and (4) associated data that allow Internet-enabled functions, e.g., IP addresses, usernames, and friend lists [32]. Unlike many other consumer technologies, VR collects these sensitive data that are indispensable for its core utility – immersive experiences [33]. Specifically, users have to trade their motion-tracking data for the full-body tracking experience; the data collected via external-facing cameras for detecting obstacles around; and voice data for social experiences [7]; just to name a few. Due to the unique immersive nature of VR technologies, researchers have been calling for policymakers to reform existing privacy laws and policies such as COPPA [34] and HIPAA [35] that would unnecessarily limit users' experiences of VR technologies [7].

In addition, a 2018 study has revealed that VR developers considered VR privacy policies problematic for providing developers with limited standards and guidelines regarding S&P [6].

In the context of social interaction, more S&P risks have emerged as VR evolves to become a popular form of social technology [13], [36], [37]. Mainstream social VR platforms, including VRChat, Horizon Worlds, Rec Room, and more, allow users to socialize with others through head-mounted displays (HMDs) [38], [39]. In this vein, a volume of social VR work has identified numerous privacy and safety risks. Maloney et al. [13] have found that social VR users tend to feel comfortable and safe to share emotions and life experiences due to the anonymity afforded by social VR. In addition, users' physical traits, such as their voices and real-life appearances, can also be disclosed since (1) voice chats are ubiquitous in social VR and (2) some users prefer to represent themselves with a virtual avatar that looks similar to their appearance in real life. More recently, with the increasing popularity of social VR streaming, users' privacy has been violated by streamers who broadcast in public VR spaces [36].

In systematizing VR threats from the existing literature, a recent SoK paper [40] has characterized adversary types corresponding to four data-processing entities in VR – hardware, client, server, and user adversaries. Hardware adversaries can access users' raw sensor data and manipulate information provided to VR applications and users. Client adversaries characterize how developers of VR applications and content creators may convey "misinformative, manipulative, and deceptive content" to users. Server adversaries can enable multi-user functionality and process networked data presented to users. Finally, user adversaries represent other users in the same VR application. After characterizing this threat model, Garrido et al. [40] have pointed out that user adversarial attacks easily occur, whereas hardware adversaries are still not mature. Importantly, due to the lack of privacy policy standards and enforcement [41], server adversaries are also easily executable, inferring many sensitive data such as user demographics in a short time.

VR risks for children. Due to the age-mixed environment [3], [4], [42], children who are considered part of the marginalized community in VR often face more tailored risks, such as predators, harassment, cyberbullying, inappropriate adult content [5], [43], [44], [45], [46], etc. However, compared to such safety threats that have been widely studied, children's S&P in social VR have been much more marginalized in scholarly work. Previous studies have collectively pointed out that bystanders and parents have concerns for children's privacy as they interact with strangers in VR [3], [4]. Notably, one study has suggested VR privacy guidelines be made more straightforward to align with children's reading and literacy levels [5]. To further provide actionable S&P-enhancing recommendations, more research centered on children's S&P is needed. Since children heavily rely on parents' decision-making of their online S&P [14], [15], [16], [47], [48], a critical gap exists in

terms of parents' attitudes and knowledge around children's S&P in VR.

Parents' risk mitigation strategies toward technologies at home. Nissenbaum defines privacy as "neither a right to secrecy nor a right to control, but a right to appropriate flow of personal information." [49]. This definition is especially applicable to online social contexts where privacy risks arise from self-disclosure [49], [50], [51], [52], [53], [54]. When self-disclosure occurs online, privacy is about the appropriate flow of information [55]. With children's significantly increased online activities [56], [57], [58], more unexpected information flows have raised new privacy concerns [16], [59]. For instance, information disclosed via email can be retained longer than face-to-face communication [16]. It is critical to protect children's privacy online since (1) privacy is an important space for children to practice their decision-making, create boundaries, and foster independence [50], [55]; (2) privacy can benefit children's experience in identity play, relationship building, and peer communication [16], [60].

Security is another important aspect of children's interactions with technology. Prior work suggests three goals of information security [16], [61]: (1) maintaining the integrity of personal information stored and transmitted through networks, (2) authenticating users with access to personal information, and (3) preserving the confidentiality of personal information. This work uses the above-mentioned definitions of S&P to unpack parents' risk perceptions and mitigation strategies.

Given the importance of S&P for children's technology use, parents have the responsibility in protecting children's digital S&P at home [62], [63]. Kumar et al. [16] have found that children aged 9 years old or younger are most likely to seek help from parents when confronted with unknown risks online and largely rely on parents' explicit rules to deal with their digital S&P risks. Other research in this vein has suggested that children of different ages trust their parents' S&P protections and guidance such as on data sharing [62], [64], [65]. Additionally, another line of research has suggested that parents' S&P attitudes and practices may shape that of children's [17], [18], [19], [21], [62], [66], [67]. For example, Shin et al. [17] have reported that parents who self-identify as more S&P-focused also tend to better direct children's S&P behavior online.

Parents adopt a variety of strategies to mitigate the risks of children's technology use [16], including talking to children, viewing children's accounts, using parental controls, being around their children during their technology use, setting rules and boundaries, etc. [20], [21], [68], [69]. Having examined different parental strategies, Wisniewski et al. [22] have summarized three types of strategies in the Teen Online Safety Strategies (TOSS) framework: (1) passive monitoring, (2) rules and restrictions in usage, and (3) active mediation such as through having conversations with children. However, when mitigating the risks, parents face a number of challenges, such as underestimating the potential risks faced by children [23], [70], [71], undermining parent-child trust [23], [72], [73], [74], and an incomplete understanding of technologies compared to their children [23], [24], [75]. Therefore, it is crucial to investigate parents' S&P practices around children's technology use at home and identify the tradeoffs in their decision-making to help parents and technology designers work together towards safer and more inclusive technologies for children.

3. Methods

Recruitment. In July 2023, we advertised our study on VR-related Discord servers, sub-Reddits, LinkedIn, and Facebook groups. Prior to the advertisement, we obtained permission from all the channels' moderators, admins, or owners. In addition, one of the researchers reached out to a local school via personal connections. After we obtained the approval from the school, we advertised through the school's official email communication. When advertising our study, we did not specify our S&P focus because we did not want to prompt our participants prior to the interview. We were interested in what concerns would first occur to parents in a natural response without preparation beforehand. Similar to Kumar et al.'s [16] approach, we framed it as an investigation into parents' perceptions and practices of children's VR usage. In our advertisement posts and emails, we attached a link to the pre-screening survey and asked all interested candidates to fill out the survey.

Eligibility and pre-screening. To qualify for our study, participants must be (1) adult residents of the US, (2) a parent or legal guardian of a child, and (3) in possession of a VR headset in their household. The remainder of the pre-screening survey consisted of questions about parents' and their children's VR usage, including purposes of usage, VR headsets, and apps that they use. We then asked them basic demographic questions, including parents' and their children's age ranges, genders, ethnicities, and parents' highest degrees. We closed the pre-screening survey with email collection for further contact.

Based on the responses, we sent out interview invitations to qualified candidates on a rolling basis until we finished 20 valid interviews. In particular, we excluded candidates who or whose children had never used VR, e.g., only the candidate's partner had used it. In doing so, we attempted to interview participants with more experience in VR and mediation of children's VR usage.

Interview procedure. We emailed each participant one day before their scheduled interview to confirm their consent to participation. To verify the authenticity of participants, we began our interview by asking participants to show their VR headsets on camera. As a result, there were nine no-shows or withdrawals from participation. After each no-show or withdrawal, we emailed them to confirm if they would like to reschedule. Meanwhile, we sent out new invitations to other qualified candidates from our survey.

From July to September 2023, we conducted one-hour remote interviews via Zoom. To address our RQs, each interview consisted of four major sections.

First, to have a better context building on their pre-screening responses, we asked participants to have a more detailed account of their children's and their VR usage. Then, we asked them about their perceptions of the general risks and benefits of children's VR usage. We did not ask participants about their S&P-specific perceptions and practices until the next section, because we wanted to see if they would raise any S&P risks on their own initiative. If not, we were curious about their primary concerns.

Following this section, we explicitly informed participants of our S&P focus and asked them to specify any S&P concerns they had. Additionally, we asked participants about their perceived stakeholders and each stakeholder's responsibilities in addressing their concerns.

Last, we asked participants what strategies they had adopted to address the concerns, if at all. We also asked them about their satisfaction with the existing S&P controls in VR and their desired features in future VR platforms. We closed the interviews with a live survey about participants' awareness and perceived (or anticipated) effectiveness of the existing parental controls in VR. Before participants filled out the survey, we encouraged them to express their thoughts as they looked at the questions. For all the participants who completed the interviews, we provided one 20 USD Amazon gift card.

Pilot interviews. Prior to the formal interviews, we conducted two pilot interviews to assess the interview duration and clarity of interview questions [76]. The two pilot participants were external researchers with expertise in VR moderation, privacy, and security. One of them was a parent. The pilot participants' relevant research expertise and parental perspectives helped us fine-tune our interview questions. We made sure our interview could be completed within one hour and asked them for advice on our interview protocol. When using the revised protocol in formal interviews, no participants expressed any confusion, indicating the success of pilot interviews. After the pilot interviews, we employed a post-interview survey. However, we found that a live survey using the quiz function in Zoom could be more interactive and useful in eliciting participants' holistic and nuanced thoughts on the features. Therefore, instead of using a post-interview survey, we switched to a live survey as a think-aloud protocol [77].

Data collection and analysis. We hosted the pre-screening and compensation surveys using Qualtrics [78]. All the interviews were audio-recorded and transcribed in English using the auto-transcription service provided by Zoom. One researcher carefully checked the accuracy of each transcript prior to the start of the analysis.

Following Saldaña's [79] coding approach, we conducted an in-depth thematic analysis of our interview transcripts. First, two researchers coded three transcripts independently. After discussing and incorporating the codes, we created an initial codebook that the two researchers agreed on. Using the initial codebook, one of the researchers coded ten of the remaining transcripts, while the other coded the other seven. Similar to many other qualitative S&P

studies [80], [81], [82], the two researchers discussed the codes and resolved any conflicts through several weekly meetings. During our analysis, as we prioritized our primary goal to generate emerging themes and concepts, we did not calculate the inter-rater reliability (IRR) to seek theoretical agreement [83].

We created codes about parents' concerns for children's VR activity (e.g., privacy-related, physical health), parents' mitigation strategies (e.g., proactive verbal education), and parents' perceived responsible stakeholders (e.g., VR companies, parents). Then, we merged similar codes and categorized them into emerging themes and sub-themes. Eventually, our codebook consisted of 13 themes, 95 sub-themes, and 613 codes. All the study artifacts, including the final codebook, can be retrieved from Appendix B.

Ethical considerations. This study was approved by the Institutional Review Boards (IRB) of all participating institutions. No personally identifying information was collected from participants. All audio recordings were transcribed and further de-identified immediately after the interviews. We also confirmed participants' consent to participation prior to the interviews and reserved their rights to withdraw at any time. During all stages of data collection, including the pre-screening surveys, interviews, and compensation surveys, participants had the right to withhold any information.

Limitations. Given our focus on parents' role in children's S&P in VR, we only interviewed parents. We must admit that parents' opinions could be skewed without children's input. However, prior work with a similar scope on parents' technology mediation also adopted this approach out of ethical considerations [4], [23]. Interviewing children and parents from the same family might lead to problems such as intruding on children's privacy from parents, embarrassment and conflicts between children and parents, etc. [4]. Considering the ethical conflicts and our focus, we chose to interview only parents and call for future work to investigate children's S&P perceptions and practices in VR.

As is typical with qualitative studies, our recruited sample size was relatively small. The study relied on participants' self-reported information, which may be subject to social desirability bias. In addition, we did not calculate our IRR. As a consequence, our findings may not be generalizable to all parents of children who use VR. To mitigate this issue, our recruitment was on a rolling basis as mentioned earlier. We summarized the key insights after each interview. Based on the guidelines from prior work [84], [85], we identified data saturation after the sixteenth interview, i.e., no more new insights emerged. We then stopped inviting more candidates other than the ones that had already been scheduled. As a result, we conducted four more interviews after identifying saturation, in line with recommended practices [85]. In doing so, we attempted to cover as many diversified perspectives as possible for an interview study.

ID	Age	Gender	Race	Child Ages	Child Genders
P1	55-64	M	White	/	F
P2	35-44	M	White	6-7,8-9	M,F
P3	45-54	M	Asian	14-15	M
P4	25-34	F	Black	6-7,12-13	M,F
P5	35-44	M	White	12-13	M
P6	45-54	M	/	12-13	/
P7	45-54	M	White	8-9,10-11	M
P8	55-64	M	White	16-17	M
P9	45-54	F	White	10-11,12-13	M,F
P10	45-54	M	Asian	10-11,14-15	M,F
P11	45-54	M	Black	10-11	M
P12	45-54	M	Asian	/	M
P13	45-54	F	White	12-13,14-15	F
P14	45-54	F	Black	12-13,14-15	M,F
P15	25-34	F	White	8-9	M,F
P16	45-54	F	White	16-17	M
P17	45-54	M	Asian	8-9	F
P18	35-44	M	White	16-17	M
P19	45-54	M	Black	16-17	F
P20	45-54	M	White	12-13	M

4. Findings

Parents' demographics. Among the 20 participants (see Table 1), six participants were female and 14 participants were male. The age ranges of participants included 25-34 years old (2), 35-44 years old (3), 45-54 years old (13), and 55-64 years old (2). Participants self-identified as White (11), Black or African American (4), Asian (4), and one participant preferred not to say. In general, parents were highly educated with a bachelor's (6), professional degree beyond bachelor's (1), master's (9), or doctorate degree (1). One participant had an associate's degree and two participants had no college-level degrees.

Although we did not require participants to specify their occupations, many of them disclosed the industries where they worked at the time of the interview, especially those working with VR/AR technologies and valuing S&P of technologies. Among the 15 participants who disclosed their professions, seven participants worked in technology companies, many of which focused on VR/AR technology and/or valued the S&P of their products. Two participants worked in finance and also had some expertise in S&P. Three participants were K12 educators who had used VR as teaching materials or worked in education technology companies. One participant was a game streamer with abundant experience in VR. The varied experiences of our participants provided us with rich and diversified insights into how parents from different industries and backgrounds approached their children's S&P in VR. The VR usage details of our study participants and their children are included in Table 2 in Appendix A. The full demographic details are specified in Table 3 in Appendix A.

In-home VR ownership and parents' usage. We only interviewed parents who had VR devices in the household. We asked participants to self-describe the VR devices they own in the pre-screening survey and verified the ownership at the beginning of the interview (see Table 2 in Appendix A). Almost all participants (17) only owned one VR headset shared with other family members, including children.

In the pre-screening survey, parents selected their purposes of usage as gaming (16), creativity (8), socialization (8), education (8), streaming and films (7), health (6), and productivity/work (4). During the interviews, we also asked participants how frequently they used VR. Seven participants reported their frequency to be on a daily basis, eight participants were on a weekly basis, three participants were on a quarter basis, and two participants were not actively using VR at the time of the interview but indicated their children were more active users.

Children's demographics. Considering children's privacy and the focus of this study, we only asked parents to report the basic demographics of their children and information relating to their S&P concerns in VR. As shown in Table 1, 10 children were female and 15 children were male. The age ranges of children included 6-9 years old (6), 10-13 years old (11), and 14-17 years old (8). Therefore, while most VR products are designed for users aged above 13 [86], [87], [88], most children in our sample (17) were below the recommended minimum age for VR usage.

As children of different ages may face different risks in VR, we paid attention to how the age of children may impact parents' perceptions and practices that are closely tied to children's S&P in VR. Therefore, in our findings, we frequently compare parents of children above and below the recommended age for usage, focusing on their different S&P concerns and strategies, if any.

Children's VR access and usage. Regarding children's VR usage, we first asked participants if they gave their children access to VR headsets. All participants said their children had used VR headsets, with varying frequencies. 10 children used VR on a weekly basis, 13 children used VR on a monthly basis, and two children were no longer interested due to the weight of the headset or motion sickness. While most parents (18) said they shared VR headsets with their children, two parents with children aged 14-17 years old said their children had their own headsets.

As shown in Table 2 in Appendix A, according to the parents, their children's purposes of VR usage included gaming (15), creativity (3), education (4), socialization (2), health (2), streaming and watching movies (1), others or unspecified (5).

Parents' and children's socialization in VR Particularly, since many S&P risks in VR currently take place during social interaction [13], [36], [37], we also asked participants to specify their socialization experience in VR. 16 participants had at least tried social VR applications or connected with others in VR. Ten participants only met people they already knew in real life, including friends and family members. Six participants socialized with strangers in VR. Notably, one participant was a VR streamer who regularly met many new people in social VR.

By contrast, children's access to social VR was greatly restricted by parents, particularly for younger children. Only three participants whose children were aged 16-17 or 8-9 years old said their children used VR for socialization. One

participant whose child was aged 12-13 years old planned to introduce his child to social VR soon. Although most participants said their children had not used VR for socialization, they had observed children's conversations with strangers in VR, mostly during gaming sessions. For children who had access to social or multi-user applications in VR, their parents believed they predominantly or exclusively interacted with children of similar ages or people in their offline connections, e.g., family members, friends, etc.

These details about parents' and children's VR usage are crucial in understanding parents' awareness, attitudes, and coping strategies toward children's S&P risks in VR, which will be detailed in the remainder of this paper.

4.1. Parents' Perceptions of Children's S&P Risks in VR (RQ1)

Due to our interview study's small sample size in qualitative nature and our goal to highlight emerging insights as opposed to generalizability, we adopt a reporting method from a similar interview-based S&P study [89] and use their frequency terminology throughout the remainder of the paper. Instead of using exact numbers of participants, we use "none" (0%), "a few" (1%-24%), "some" (25%-44%), "about half" (45%-54%), "most" (55%-74%), "almost all" (75%-99%), and "all" (100%), when appropriate.

In response to RQ1, our findings highlight: (1) Parents generally lack S&P awareness in VR, largely due to the belief that VR is still in nascent development and therefore risks are a "future thing." (2) S&P risks are regarded as *potential risks*, whereas the influence of VR on children's physical health is defined as *real-life* risks by parents. (3) Among the identified S&P risks, parents generally have greater concerns in social interaction contexts than data surveillance by companies. Although they can name a few risks from VR companies, they generally discard such concerns in practice.

4.1.1. Non-S&P Concerns as Parents' Primary or Only Concern for Children's VR Usage.
We asked parents about their concerns toward children's VR usage without priming them with our S&P focus. As a result, almost no parents brought up concerns for S&P on their own initiative. Instead, they primarily mentioned concerns for children's physical health issues, online safety, and "bad influences."

Defining eye-sight and physical injuries as real-life risks.
When answering the question about general concerns for VR, most participants illustrated both *risk-life risks* they had perceived or experienced from their own children and *potential risks* they could imagine for other children or in future settings. For real-life risks, most participants mentioned concerns about the influence of VR on children's eyesight. As P15 mentioned, "*The only risk so far that we've had is my son needs glasses now, but we don't know if there's a direct correlation between the Oculus and his eyesight.*"

Similarly, another participant P2 directly pointed out his "real-life" concerns as opposed to "potential" concerns:

"*There's the real-life risk of running into stuff or breaking things as kids get carried away within a particular environment. I don't know if there are long-term risks. There are potential risks like data collection. Ideally, people are collecting data [in VR], but I just don't know if they are.*"

According to P15 and P2, physical injuries were defined as parents' real-life concerns. However, parents also recognized some "potential risks" like data collection that they just had no way to directly confirm.

Stranger danger in a child-adult co-existing ecosystem.
Similar to what prior work has pointed out [3], [4], [42], child-adult co-existence in VR was a major safety concern. P1 mentioned:

"*The gameplay is high-action and fun. So it really appeals to all age groups. So the kids are in there playing with both adults and other kids...I don't think that the companies are doing a good job of limiting it to just kids. They have a financial reason for wanting everybody to use their software.*"

Some participants echoed P1, indicating their doubt about VR companies' motive and capability to separate children from adult users. According to participants, the child-adult co-existence in the VR ecosystem could lead to many other potential problems, including predators and cyberbullying.

P6, an active social VR user, said, "*I suppose there could be a way you could track where they (children) were actually if the person was a potential predator. I'm sure there's a way to track the IP of a VR device.*" P6 had heard of predators collecting IP addresses in social VR, and like some other participants also mentioned, they would be afraid of children being lured to meet online strangers in person, either voluntarily or involuntarily.

Besides predators, participants also mentioned that in an anonymous and immersive environment, cyberbullying could be common and more realistic. As P2 noted, "*My largest concern would be, the potential for bullying within open environments where you can encounter cyberbullying, particularly with the potential lack of supervision.*" Like P2, some participants were well aware of the anonymity afforded by avatar-mediated communication [45], [90], [91]. They perceived anonymous environments like VR to be a place where cyberbullying was more likely. Worse yet, as P11 stated, "*[c]yberbullying becomes more visceral in VR (compared to text-based cyberbullying).*".

Vigilance toward "bad influences." Besides safety concerns, another frequently mentioned concern was some bad influences from other VR users and the environment designed chiefly for adults.

The first major type of bad influence was bad language in VR observed by participants. A few participants said they had witnessed their children and other children use a lot of bad language, e.g., curse words, racial terms, etc. For instance, participant P16 stated:

"*I don't like a lot of foul language when they're playing. So that's the one thing I've monitored. If they're playing*

with people who are using foul language, I tell them to get off."

Besides the under-regulated bad language, the age-mixed environment in VR also brought in the problem of inappropriate content, which has been documented in existing literature [3]. Participants, especially those with social VR experience, said that the user-generated worlds were a big issue. Similar to the perception that VR companies did a bad job limiting the age group of users, participants also thought the mechanism of allowing users to upload their own worlds could potentially introduce children to content that was not designed for them.

Importantly, however, participants also noted that bad influences were not only from adults but also from other children who used VR without parents' monitoring. P14, who did not have much social VR experience, said she could imagine "*kids in VR might have families who have a different or opposite thought process from us.*" Therefore, P14 was very concerned about the "*bad influences*" from other kids in VR.

P14's concerns could be testified by prior work that reported children's bullying behavior in VR [3]. Toxic behaviors by children were also spotted by other participants with social VR experience. According to P1, "*For a few times in public worlds, I've seen that it is obviously fairly young children turned loose in this environment and not being monitored.*" Echoing P1, P19 even blocked some children in VR. "*I've learned how to kind of block some children, because it was just, you know, so freewheeling that some children feel like they're uninhibited enough to do anything because you can't see them.*"

In summary, parents were concerned about different types of bad influences from a variety of actors in VR, including adults, children, and user-generated environments.

4.1.2. S&P Concerns in Social Interaction Outweighed Data Surveillance. After asking participants about their general concerns, we specified our focus on children's S&P in VR. About half of the participants said that they had never thought about the S&P issues in VR before. After being prompted, participants were able to name some S&P risks given their prior experience with other technologies. However, some participants would emphasize such concerns hardly occurred to them during children's VR usage. In comparison, while some participants working in technology or S&P-related industries were more concerned about data surveillance from companies than self-disclosure in social interaction, most of the other participants were more concerned about children's self-disclosure in VR. Mapping this finding to the threat model suggested by Garrido et al. [40], we suggest that parents with more S&P experience are more concerned about hardware and server adversaries. Still, most parents are much more concerned about user adversaries.

Parents showed awareness of headsets' and apps' data collection risks but discarded the concerns in practice. For data S&P in VR, most parents mentioned their concerns for biometric data collection and analyses for user profiling

and advertising purposes. Intriguingly, many children and family studies on S&P-related issues with technology have found that families easily neglect commercial data mining and surveillance in their S&P mental models [16], [62]. Our findings, however, show some progress that families have made in developing awareness of surveillance capitalism, as our participants covered the four sensitive data types according to Dick [7], including observable data, observed data, computed data, and associated data in VR (see Section 2). For example, P20 said:

"[E]ye-tracking would be a big concern of mine. From an advertising and psychology perspective. How people think and what they're looking at are correlated. We would only use products that use eye-tracking internally for system software purposes only."

For participants like P20, cutting-edge technology such as eye-tracking could collect physiological and behavioral signals, which could be more invasive compared to their smartphone activity. Echoing P20, P18 mentioned, "*I would imagine there's a lot more data that comes in when somebody's interacting with VR, so I think the biggest privacy risk is how much neural information you are giving up.*" Besides "*neural information,*" participants were also concerned about their voice data being collected by companies, due to the expansion of AI that could be used to fabricate and manipulate voices.

Importantly, even though participants were aware of the potential data collection and inference by VR companies, they generally discarded such concerns in their parenting practices. As P1 highlighted,

"I'm more worried about their interactions with strangers than I am worried about advertisers...There are all kinds of people talking about how eye- and face-tracking can allow companies to know more about you...But I don't know what they are going to do with it that we're worried about. I have never found an answer."

Although P1 acknowledged the risks of data collection and inference by companies, he believed that those risks were still very abstract and theoretical to laypeople. He added, "*A lot of people are doing a good job of presenting these pieces are scary but not doing a good job of telling me why they're scary...But you know the risk of someone knowing your information.*" We also noticed that a lot of what other participants described as VR data S&P risks testified to P1's opinion. Participants knew that VR users gave out their biometric data but could not describe the consequences. However, they were able to accurately demonstrate example consequences (as detailed below) of children's self-disclosure in VR.

Children's self-disclosure in immersive environments was much more alarming. Participants considered self-disclosure a huge risk for two main reasons: (1) It is hard for children to understand the publicity of having conversations in VR. (2) The nature of immersive environments and "*cute avatars*" might trick children into giving out information as naturally as talking with friends in person.

Participants with multiplayer or social VR experience reported their experience encountering children voluntarily giving out information in public worlds. P1 said, "*If you were playing a game with a kid who knows a credit card number, they would probably just tell you the number. That's hypothetical but I've seen many kids volunteer that sensitive information in VR.*" P5 mentioned:

"In my experience, it doesn't take much to know a kid's private information. Sometimes when I go into rooms, I see kids share all the information publicly and voluntarily...Kids don't understand that it's just like standing on the street corner and shouting it."

For P5, the publicity of conversations in VR is hard to be perceived as risky by children as personal information disclosure is too common in VR.

In addition, some participants attributed children's self-disclosure to the immersion and avatars. P20 said, "*Feeling immersed in VR might make it a more likely scenario where children might disclose something to someone behind an avatar.*" Compared to data collection and inference by companies, participants could describe self-disclosure risks in VR in a much more vivid and specific way. They also considered such risks much more "*direct*", despite acknowledging the subtle and potentially long-term risks of data surveillance in VR.

4.1.3. Reasons for Lack of Concerns: Being "Cutting-Edge" and "Harmless". Interestingly, most participants said that they were not concerned about their own children's S&P in VR at the current stage because VR was still a "*privilege*" and there were not many users in it to worry about, especially compared to other more mature technologies like social media. Most parents of teenagers (aged 13-17) also expressed their trust in their children's maturity in using technology. As a result, participants generally lacked S&P concerns in practice, and therefore did not enforce many mitigation practices.

Parents lacked the motivation to fight a future thing. Some participants mentioned that VR was still a privilege in its infancy. For this reason, participants considered VR much less risky than some other technologies that are being used by a majority of people. As P20 explained,

"I'm way more concerned about social media...There's not a whole lot of critical mass yet in VR, so things will probably change when everybody piles in."

Similarly, a large portion of participants mentioned that the risks they identified would not be concerning until some point in the future when VR technology becomes much more advanced and popular than its current state. VR risks are not "*well-defined*" at this point, as P1 said:

"The privacy problem in VR is more of a big future thing as they're getting more and more information sometime in the future. It's still a problem that's very nebulous and not well-defined. So I have a hard time being motivated to fight it."

P1 showed a state of mind that is inconsistent with his VR parenting practice, demonstrating *privacy paradox* [92],

[93]. Privacy paradox refers to the discrepancies between users' expressed privacy concerns and their actual behavior. In our context, even though P1 knew the risks existed, he still had little motivation to mitigate them in practice.

As a result, participants usually focused more on their children's use of other technologies like social media, neglecting the harms of VR as a "*future technology.*"

Trust in children's maturity in technology use. In addition to defining VR risks as a future thing, some participants, especially those who were parents of teenagers (aged 13-17), said that they were not concerned because their children were tech-savvy and mature in their S&P decision-making. As P14 said, "*I think at this point for him. He's kind of on his path to becoming an adult. So I've given him advice, and I'm kind of trusting that he's gonna follow it. He's fairly mature for 16.*" Similarly, other parents of teenagers echoed P14 and believed their children's familiarity with VR to have surpassed theirs.

Some participants who were experienced in VR said that they suspected most other parents would have bought VR just to babysit their children without having any knowledge of VR. As P1 said, "*I don't think parents understand that there's a shift there. It goes from being something that's happening on a screen in front of you to something that is happening to you.*" P1 assumed that many parents would consider VR the same as many other technologies like phones, TVs, and tablets.

Indeed, when other participants discussed some risks of VR, they would reference more common technologies, like what P14 (a parent of teenagers) argued, "*the risks are pretty much the same in any type of technology.*"

Some participants not only neglected the nuances between different technologies, but they also regarded VR as a kind of video game that was just the same as being played on a PC. Interestingly, participants were generally much less concerned about their S&P when in gaming contexts. As P16, a parent of a teenager nearing adulthood, explained why she did not worry about her son's privacy in VR, "*I am not concerned because they're just in this game mode. There's nothing personal involved.*" For some participants like P16, gaming sessions were mostly about play and involved very few privacy risks.

In contrast, parents of children at younger ages (below 13) in our study, such as P2, P7, and P15, showed more vigilance toward VR risks. Most of the parents discussed that they changed or planned to change their strategies as children grew older. Consequently, some parents of older children, especially those nearing adulthood, might be more neglectful of VR risks compared to those of younger children. In general, parents of older children demonstrated an even more imbalanced understanding of VR compared to their children.

Such information asymmetry about technology between parents and children has also been widely documented in existing literature [23], [24], impeding parents' ability to engage in teens' technology use.

4.2. Parents' S&P Risk Mitigation Strategies (RQ2)

Following Wisniewski et al.'s TOSS framework [22], our findings highlight: (1) Parents primarily rely on active mediation, rules, and restrictions in usage. (2) Parents generally consider parental controls in VR important but face significant technical constraints. (3) In mitigating S&P risks, parents have to navigate complex tradeoffs between autonomy, safety, and S&P.

4.2.1. Active Strategies as the Primary Strategy: Proactively Mitigating Risks via Conversations and Rules. We asked participants what steps they had taken to address the concerns they had, and almost all participants mentioned proactively educating children through conversations and setting rules. However, most of them also emphasized that these conversations and rules were not exclusive to their VR usage. Hence, the ineffectiveness of such strategies in certain VR contexts might have been neglected.

Parents emphasized online S&P issues to children, but not specific to VR. For most families we interviewed, participants claimed that they valued online S&P education for their children. Having enough conversations about online S&P was also one of the reasons why participants were not concerned. For instance, P14 said:

"I put some rules down for my kids, and they've been pretty good about it. We've had discussions like, we don't put any of your personal information out there. We don't share real names, ages, birthdays."

Participants like P14 who said they had strict rules and open conversations with their children all claimed that their children followed their guidance well. However, P14 also emphasized that their rules were *"pretty much the same across any kind of electronic communication that can go outwards."*

While participants seemed to be generally confident and satisfied with their approach, P7, who had more VR expertise was opposed to this approach and believed that some physical references should be in place when educating children about S&P in VR:

"We've had those conversations in the context of physical interactions. That makes more sense to kids. When they get on VR, in their head, they're in a safe video game space. They're not thinking, oh, that cartoon character could actually be a person who has ulterior motives like a stranger on a street."

According to P7, although parents might have had sufficient privacy education in general digital communication, the proximity between VR and real-life interactions makes it more reasonable to set physical references in their VR privacy education, as opposed to sharing the same set of rules across all digital communication in general.

Managing children's app access and S&P information flows in VR through shared and associated accounts. Unlike social media usage where children usually have separate accounts from parents [94], most participants shared the only set of VR headsets and accounts with their children. While this practice was not out of mitigation considerations, some participants indicated that sharing headsets and accounts helped them better manage children's VR activity, including their access to certain apps. For example, P14 mentioned:

"My kids' accounts are linked to my email, so they have to go through us to buy an app. I can also see any kind of activity. Everything comes to me via email. So I still have a little bit of insight."

In some cases, participants made sure to be present when their children tried to create accounts in case they provided excessive information for platforms. As P10 noted, *"I'm concerned about the phone number and other family information going out. That's why I keep my kids away from creating accounts on their own without having us know."*

Hence, sharing accounts or creating ones under parents' supervision was a proactive strategy for parents to not only manage children's app access but also their information flows in the VR ecosystem.

Notably, this approach was more discussed by parents of children aged below 13. For parents of children aged above 13, almost all of them did not mention managing or sharing accounts with their children. A few of them mentioned that they would only occasionally check their activity (e.g., interactions with other users) without overly intruding on children's privacy. In addition, the only two participants whose children had their own headsets were aged above 13, further indicating that parents of teenagers may have fewer restrictions and monitoring over their VR usage. This shows a gap where parents of children aged above 13 have limited concerns and mediation toward their children's use of VR products that primarily encourage users aged above 13 [86], [87], [88].

4.2.2. Challenges in Passive Strategies: Technical Issues & Parents' Frustrations. According to the TOSS framework [22], monitoring and parental controls fall under passive mediation. Our study uncovered that parents faced a range of challenges in their passive strategies, including parents' technical frustrations and children's workarounds.

Maintaining *ambient awareness* [1] as the most common monitoring strategy. Almost all participants said they would occasionally check in with children when playing VR, making sure to be able to hear the conversations. In addition, for physical safety considerations, most participants would ask their children to play in open areas like the living room. For example, P11 said:

"They basically play in the living room and I'd make sure the volume is loud enough to hear some of the stuff that's being said."

However, unless VR is cast on a screen, participants would not be able to see what their children do. While paying attention to the sounds is also a more common option

---

1. Referencing [16], we use this term to indicate parents' casual monitoring when they are nearby their children during technology use.
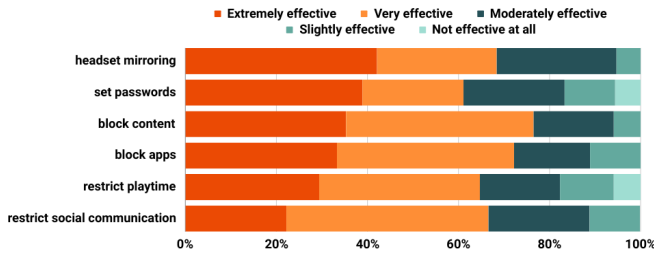
Figure 1. Participants' ratings for the anticipated effectiveness of each parental control feature in VR.

for parents who monitor children using 2D media [16], VR was much less flexible for our participants who would like to visually check out their children. This constraint influenced parents' practices and attitudes toward different parental controls in VR, as we discuss below.

Parental controls in VR were important but posed technical constraints. In the last section of our interviews, we asked participants to first indicate if they knew the feature, and then rate their anticipated effectiveness of each parental control that we found in mainstream VR products.

As a result, 75% of participants had heard of setting passwords, 70% had heard of blocking apps, 65% had heard of headset mirroring and playtime restrictions, 60% had heard of social communication restrictions, and 55% had heard of blocking specific content. While this result shows that most participants had heard of these parental controls, their qualitative feedback demonstrates that they had very little experience setting up these controls in practice. For example, P20 said, "*I don't think I've used parental controls, although I would kind of assume they exist.*"

Some participants like P20 also said that they had never tried setting up parental controls, but given their experience in other technology mediation, they assumed they would be able to set them up.

For the anticipated effectiveness (see Figure 1), overall, headset mirroring was rated as the most effective feature. As mentioned, without casting VR on a screen (i.e., headset mirroring), parents would not be able to visually check out their children's VR activity. Consequently, headset mirroring was rated as the most effective. However, participants who tried headset mirroring highlighted its major drawbacks, including technical issues (e.g., high latency and connection issues) and low engagement for parents. Specifically, two participants said they discontinued the use of headset mirroring because of the unstable connection. For engagement, some participants questioned headset mirroring because they believed it would be unrealistic and not engaging for parents to keep watching children for a long time. As P8 said,

"*I'm not participating in anything (when looking at the headset mirroring). I'm simply there observing and spectating. So it's of course, not an engaging experience for me. I would rather be doing something where we could do it together. But we don't have a second headset.*"

Besides headset mirroring, blocking apps and blocking content were also highly rated, due to their preventive nature favored by some participants. However, a few participants

also pointed out the limitation. As P17 mentioned, "*Blocking is not going to be effective. There's always going to be something that you don't know about.*"

To our surprise, while social communication was the most concerning privacy risk to participants, restricting it was not the most effective feature for participants. As P18 explained, "*I mean, it's a question that, if you want your child to be able to communicate socially, it'll be a kind of an all-or-nothing thing.*" While restricting social communication could prevent children from interacting with strangers, it was also perceived as too limiting and could not "*help them learn to do things in the correct way.*" (P18). Indeed, passive mediation means stopping children from doing certain things and hindering their chances of learning in practice. Navigating such tradeoffs between children's S&P and their autonomy was a hard process for our participants (as detailed in Section 4.2.3). In general, we observed that parents of children aged above 13 were more against the idea of using passive features that could hinder children's autonomy. Hence, some parental controls were much less important to parents of children aged above 13. On the other hand, parents of younger children favored these features for their effectiveness in protecting children from harms.

For passwords and playtime restrictions, while participants found them effective in directly stopping children from accessing VR, they also noted two main drawbacks that discouraged them from using the two controls: (1) By experience, children are likely to work them around and (2) these two controls are too passive while increasing parents' workload, e.g., having to unlock the headset whenever children want to play.

4.2.3. Complex Tradeoffs Between Autonomy vs. S&P.
One major discussion we had with our participants was how they weighed and balanced their S&P mitigation practices and children's autonomy in VR. Participants held two different stances: 1) Some participants would rather trade autonomy for children's S&P in VR, while 2) most participants advocated for more active approaches to support children's autonomy, even at the cost of potential safety and S&P risks.

Participants who preferred to trade autonomy for children's S&P in VR considered the latter more important mainly for two reasons. First, the current VR ecosystem is largely designed for adults, and children are more likely to get into inappropriate situations at this point than later when VR becomes more mature. Hence, it is still too early to give children too much autonomy. Second, VR is still a very minor part of most children's lives, and therefore they have plenty of opportunities to maintain their social autonomy elsewhere, e.g., physical interaction contexts, smartphone usage, etc. As P1 noted:

"*Today we've gotten to the point where having a phone and a tablet is necessary for you to be on par with your peers...VR is not that way right now...Kids have plenty of other places where they can have autonomy in social experiences...Today, I don't see any problem with VR being completely restricted.*"

On the other hand, participants who advocated for children's autonomy even at the cost of safety and S&P believed it would be more important for children to gradually learn to tackle harmful situations with parents' guidance. Using passive strategies would hinder children's chances of learning in the real world where parents cannot always keep them company.

Consequently, some participants advocating for the second stance claimed that parents could only help them understand and prepare for potential risks beforehand, whereas when real risks took place, they had to count on themselves with more effective moderation or defensive mechanisms to be in place – a gap that VR companies have the responsibilities to fill (as detailed in Section 4.3). Importantly, most participants also emphasized that the balance between autonomy and children's S&P and safety in VR would be a dynamic process where the significance of one and the other might be constantly changing in the long run of children's development. Specifically, almost all of the participants who valued S&P over autonomy had children aged below 13, whereas almost all of the participants whose children were aged above 13 valued autonomy more. This shows the role of children's age in impacting parents' decision-making when facing the autonomy-S&P tradeoffs.

Overall, parents of children using VR might have to deal with a series of complex and dynamic tradeoffs when trying to mitigate S&P risks in VR. This finding echoes prior work that suggests managing children's technology is like other daily activities where parents' strategies might be changing in a "*complex, contextual, and dialectic process.*" [16], [95].

4.3. Responsible Stakeholders and Desired S&P-Enhancing Features (RQ3)

We asked participants to describe the responsibilities of different stakeholders and features that they desired to enhance children's S&P in VR. Our findings suggest: (1) Participants generally agree a multi-stakeholder ecosystem must be established to make concerted efforts towards more S&P support for children using VR, with parents being the most accountable stakeholder. (2) While participants desire several features including real-time feedback and alerts with regard to children's S&P in VR, they also have reservations about VR companies' data surveillance.

A multisided VR ecosystem towards more S&P support for children. When naming perceived stakeholders and their responsibilities in mitigating S&P risks for children's VR usage, all participants suggested more than one stakeholder. Taking all participants' opinions together, we summarize four main stakeholders – parents, VR companies (including headsets and apps), governments, and schools/educators.

Among the four parties, parents were identified as the most accountable. Some participants expressed their concerns for adults' lack of S&P understanding in VR. For instance, P1 mentioned, "*From what I've seen online, there are a lot of parents handing their kids the VR without even*

trying VR for a few times. As long as the kid is being quiet and entertained the parents aren't paying attention." To understand the potential risks in VR, participants with more VR experience highly suggested other parents also experience VR, preferably with their children together. For example, P14 demonstrated how she tried VR with her children for the first time:

"Let's do it together the first time, so we can see, like what kind of experience and things we need to look out for...Just so we know some potential bad experiences."

P14 said it would be essential for parents to go over the first-time VR experience, gaining some firsthand insights into the potential risks. In doing so, children would be more prepared when harmful situations take place.

Another gap exists in parents' understanding of the S&P practices and policies across different VR products. We asked our participants if they had ever read any privacy policies on VR platforms, and almost all of them answered no, including those with more relevant expertise. This was in part due to the low readability of the policies, but also because of the inaccessibility of reading them through the headsets.

VR headset manufacturers and app companies (we combine them into "VR companies" in this paper) were also considered largely responsible for mitigating the S&P risks. In our interviews, a few participants expressed their concerns about the conflicts between users' privacy and companies' business models. In general, they believed that most of the existing S&P-enhancing efforts were primarily for promoting their public image. Correspondingly, prior work has also documented the trade-off that companies face between protecting children's privacy and sustaining their business models [96], [97], [98]. To mitigate this concern, our participants suggested making S&P guidance part of a mandatory step before the use. As P18 suggested, "*I'd prefer if it was in plain language with some short mandatory steps like watching a video... These steps should be very upfront.*" Making privacy guidance shorter, clearer, mandatory, and upfront would be parents' preferred practice, showing the company's real effort in making the products more S&P-centered.

Nevertheless, as participants noted, it would be hard for companies to implement such practices as they might conflict with their business models. It would be unrealistic to only count on companies and expect them to be all moral without regulations. Hence, our participants believed that legal regulations must be in place by government bodies to enhance supervision over VR companies' S&P practices.

Last, as a few participants pointed out, as VR becomes more and more prevalent, schools and educators also have the responsibility in teaching children about the nuances of data surveillance and self-disclosure in VR, compared to other technologies.

Parents' desired features and S&P considerations. The desired features mentioned by participants included (1) real-time S&P alerts and feedback when harmful interactions take place, (2) AI-based harm detection, (3) a secondary app

in place of headset mirroring, and (4) a general usage report sent regularly, e.g., weekly reports, summarizing children's basic VR activity.

As noted by participants, most of the existing moderation and defensive mechanisms in VR are reactive, e.g., blocking and reporting. However, going through the process of blocking and reporting was perceived as "worthless," as it would not make up for the damage and would take too much time to receive feedback. As parents, our participants preferred to know immediately if harmful interactions were taking place. Participants who were concerned about bad influences also hoped to have red flags or alerts sent to them, e.g., an indicator of bad language. However, these ideas also raised some other participants' concerns, mainly for companies' data surveillance. As P18 explained:

"While that (real-time alerts) sounds like a really good idea, that would pretty much just be automatically consenting to a hundred percent monitoring of everything that's being said."

According to participants, the same concern also applied to AI-based harm detection and secondary apps, all sounding helpful for parents in managing risks more effectively at the price of volunteering more sensitive data to companies.

A few participants proposed an alternative – sending parents reports with only basic but essential information. In doing so, participants were still able to get an insight into their children's usage while not risking too much of their privacy. As participants did not reach an agreement on how this "basic but essential" report mechanism should be designed in the interview, we will further propose our recommendations in Section 5.

5. Discussion

In summary, our work has found an alarming status quo where parents of underage VR users generally demonstrate a lack of awareness regarding their children's S&P in VR due to their conception of VR being "cutting-edge" and therefore "harmless" (**RQ1**). Despite parents' lack of S&P awareness in VR, they carry out a series of general rules toward at-home technology use. Notably, when it comes to VR, parents primarily rely on active strategies as opposed to passive ones that pose significant technical constraints (**RQ2**). Finally, by prompting our participants in the interviews, they collectively demonstrate a need for a multisided VR S&P-enhancing ecosystem, with an emphasis on parents' responsibilities and expectations toward a series of S&P-enhancing features (**RQ3**). In the remainder of this section, we first discuss how our work extends or contradicts prior work. With the takeaways, we then discuss our recommendations for the critical stakeholders, including parents, educators, VR companies, and governments.

Parents' knowledge gap in VR led to their overgeneralization of S&P rules for children in diverse contexts. While prior work on children in social VR has collectively pointed out that parents have some S&P concerns for children in VR [3], [4], [5], they did not specify parents' reasons behind the (lacked) concerns and risk mitigation strategies. Interestingly, one 2018 study on VR users' and developers' perceptions of S&P in VR shows some similar findings, including prioritizing health concerns over privacy and security [6]. This shows consumers' general S&P perceptions may not have evolved drastically over the course of the past five years, urging a need to investigate more effective S&P education, features, and policies regarding VR. Our work builds on this stream of work by first revealing parents' knowledge gap in VR and how it raised S&P concerns for children, including blurring S&P rules across a broad range of contexts.

Prior work has pointed out that parents' incomplete understanding of technology compared to children might impede parents' ability to engage in children's technology use [23], [24]. As a result, parents might underestimate the amount and type of technology use and online interactions that their children engage in, hence putting them at risk [70], [71], [99]. Similarly, while bystanders in social VR have witnessed great risks for underage users [4], we noticed that parents in our study, especially those with less VR experience, claimed that their perceived S&P risks would not apply to their own children at the current stage (Section 4.1.1). Therefore, it is worth suspecting whether the parents had underestimated children's VR activity and S&P risks. Admittedly, parents' perception of VR's immaturity may be correct in some aspects, especially regarding the immature hardware adversaries [40]. Most parents without much S&P experience overlooked or disregarded server adversaries that inferred sensitive data [40]. In other words, while parents may be correct that immersive data collection had not yet been quite extensive, data inference might have been largely underestimated, according to the established threat model [40].

Parents' overgeneralization of S&P rules in all digital devices defer addressing concerns to the future. An important finding of our work is that parents overgeneralize their S&P rules across diverse contexts, including sharing the same set of rules for all forms of digital communication (Section 4.2.1). Despite the fact that parents understand the potential of extensive biometric data being collected in VR compared to other technologies [13], [37], most of them still discard the differences in practice, especially those who seldom or never use internet-enabled VR applications. We believe this phenomenon may be attributed to parents' lack of experience in using VR and their knowledge gap in the nuances between VR and other technologies. We will propose relevant recommendations for parents and educators later in this section.

Another reason for this type of overgeneralization is that parents prioritize children's S&P in other technologies such as social media (Section 4.1.1). For this reason, parents deferred addressing their S&P concerns in VR. Interestingly, in a study of children's S&P online in general (e.g., social media) [16], parents still consider S&P risks as a future concern. Therefore, we suggest that in addition to enhancing parents' understanding of VR technologies, there should

be other measures to enhance S&P education itself more effectively, such as setting physical references as accounted below.

Parents' perceived differences in S&P risks between offline and VR settings impede effective S&P education in VR. Prior work regarding other consumer technologies has pointed out that parents blur S&P rules in offline and online settings [23]. However, despite overgeneralizing S&P rules across different technologies, most parents in our study understand the shift between S&P risks in offline and VR settings, mainly due to the anonymity afforded by avatars (Section 4.1.1). Parents are concerned about children being tricked by the predators behind the attractive avatars.

Problematically, while most parents understand the differences between S&P risks in offline settings and VR, the proximity in social interaction between VR and face-to-face settings has been overlooked. Only P5 and P7 who have abundant VR experience educate their children about S&P risks in VR by setting physical references or metaphors (Section 4.2.1). All the other parents in our study primarily rely on their general rules for technology use, e.g., not disclosing privacy when chatting with people online. However, text-based communication is drastically different from voice chat in VR [45], which resembles talking to friends in face-to-face scenarios. This shows a need to set physical references or metaphors when educating children about S&P in VR. As suggested by prior work [100], [101], [102], [103], physical metaphors are important in improving S&P awareness and protective strategies. For example, food nutrition labels serve as a physical metaphor for "privacy nutrition labels," better informing users of S&P-related information [89], [104], [105].

Parents' complex tradeoffs between passive and active strategies raised questions toward S&P controls in VR. Our work extends prior work that has discussed children's autonomy and S&P in their technology use [16], [22], [99], [106], suggesting that parents navigate complex tradeoffs between children's autonomy and S&P in VR (Section 4.2.3). For example, even though parents are largely concerned about children's self-disclosure in social interaction, they consider parental controls that restrict social communication less useful because such an "*all-or-nothing*" approach would not help children learn the correct tactics in practice (Section 4.2.2).

Notably, one difference between VR and other consumer-facing technologies lies in the fact that VR has not yet "*gotten to the point where having a phone and a tablet is necessary for you to be on par with your peers,*" as highlighted by P1. Due to this perceived difference, some parents consider maintaining children's S&P much more important than their autonomy in VR. For these parents, passive strategies such as using parental controls are expected to be helpful.

However, even if parents would prefer protecting children's S&P over autonomy in VR, they are still largely constrained by the existing S&P controls in VR, due to their low usability, engagement, and granularity (Section 4.2.2).

For this issue, we will propose recommendations for VR companies later in this section.

Recommendation 1: Parents and educators can enhance awareness of technological nuances and physical metaphors in their S&P education. As mentioned earlier, parents tend to overgeneralize their S&P rules in all digital devices (Section 4.2.1). Therefore, the first recommendation for both parents and educators (public education for all and educators at school) is to enhance their awareness of the nuances between VR and other technologies that they are familiar with.

For parents, in particular, it is recommended to experience VR themselves as much as possible. It would be even better if parents could maintain their knowledge level about VR on par with their children's. Since VR is an immersive technology, the social experience and data surveillance might be completely different from what they know about smartphones, trying out VR themselves would be the best way for parents to understand the nuances. The significance of parents' firsthand experience in VR is also obvious in our findings, as participants with more VR experience demonstrated better awareness and richer insights.

A specific example is that parents with S&P experience demonstrated greater concerns toward hardware and server adversaries [40]. While the lay parents' perception of immature VR technologies may be correct in terms of data collection, their ignorance of the risks of data inference in VR is alarming. Hence, we also urge more privacy education on the different types of adversary types in VR, especially server adversaries.

The same recommendations also apply to educators. As school education has already incorporated S&P risks in social media as part of the curriculum [23], it is also crucial to list VR S&P risks in the agenda, especially for those who utilize VR as an education technology [12], [107], [108], [109].

When educating children about S&P risks in VR, both parents and educators should consider leveraging physical metaphors, as opposed to referencing other digital devices. Prior work has suggested that children might perceive physical contexts S&P riskier than online contexts [23]. It is therefore highly recommended that parents and educators set more physical references when informing children of the S&P risks in VR. For example, parents and educators can compare talking in a public social VR world to shouting out loud on a street, as P5 suggested in Section 4.1.2.

Recommendation 2: VR companies should improve the S&P controls and guidance for children and parents. Our findings also highlight that parents generally find S&P controls unusable for parents and children themselves (Section 4.2.2 & 4.3). Parents also find it hard to read the privacy policies in VR (Section 4.3). Hence, we call for VR companies to re-design their S&P controls for both children and parents, involving more *engagement, granularity, and modality-specific considerations*. Drawing on our participants' desired features (Section 4.3), we also urge
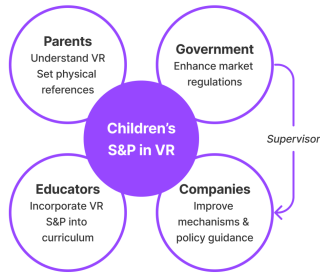
Figure 2. The recommendations for the main stakeholders in the multisided VR ecosystem for children's S&P.

VR companies to provide better S&P guidance as a part of the mandatory onboarding process.

In improving the usability of S&P controls in VR, two main problems must be addressed – (1) technical constraints such as connection issues and high latency, and (2) low engagement. Among a series of controls, parents find headset mirroring most effective (Section 4.2.2). However, due to technical issues, they also refrain from using this feature. In place of headset mirroring, parents hope to use secondary apps accompanied by the VR product (Section 4.3). The secondary app can not only replace the functionality of headset mirroring but also provide real-time alerts and other features to help parents gain more engagement while protecting their children in a more timely manner.

Considering parents' S&P concerns about these desired features, we suggest increasing the granularity of S&P controls. Specifically, since parents all have very different considerations when facing the tradeoffs between children's S&P from the company and strangers, S&P controls should enable parents to set what exact information they allow companies to collect and analyze for generating real-time or periodic S&P alerts.

In addition, almost all the parents in our study have never read any privacy policies of VR products, showing an urgent need to improve the S&P guidance for parents and children in VR. In short, S&P guidance in VR should be modality-adapted, mandatory, and engaging. Indeed, reading lengthy policies in VR can be difficult [110], and parents seldom search the S&P practices of VR products using mobile phones or PCs. Therefore, it is necessary to adjust the design of texts to align with users' reading preferences in VR, considering text lengths, sizes, color contrasts, etc. [110].

Besides valuing users' reading experiences in VR, other mechanisms include interactive onboarding tutorials to introduce S&P-risky scenarios and protective mechanisms. In particular, as prior work suggests [5], a "*straightforward and well-explained guideline*" in line with minors' literacy levels is important.

Recommendation 3: Governments should verify VR companies' S&P promises without overly hindering immersive experiences. Even though VR companies demonstrate good S&P promises through updating their policies, parents still have concerns about whether companies would fulfill the promises (Section 4.3). Therefore, it is important

for governments or law enforcement sectors to enhance auditing over VR companies' S&P practices.

On top of enforcing privacy laws to VR [10], [11], prior work has called for policymakers to reform existing privacy laws such as COPPA [34] and HIPAA [35] based on the unique affordances of VR such as immersion. While these policies may be generalized to other technologies, they could overly hinder user experiences in VR. Hence, our recommendation is also for the law sectors to enhance their knowledge of VR and iterate privacy laws for VR while supervising VR companies' S&P practices.

6. Conclusion

This study presents an in-depth qualitative analysis of parents' perceptions and practices toward children's S&P in VR. Our results highlight that parents generally lack or discard S&P awareness in children's VR usage. In mediating children's VR usage, parents currently primarily rely on active strategies such as verbal education. Passive strategies, however, have been less effective due to technical constraints. Parents also agree that multiple stakeholders are responsible for mitigating S&P risks for children, with parents being the most accountable stakeholder. To conclude, we propose specific and actionable recommendations for the critical stakeholders.

Acknowledgments

References

[1] R. Bagheri, "Virtual reality: The real life consequences," *UC Davis Bus. LJ*, vol. 17, p. 101, 2016.

[2] R. Epp, D. Lin, and C.-P. Bezemer, "An empirical study of trends of popular virtual reality games and their complaints," *IEEE Transactions on Games*, vol. 13, no. 3, pp. 275–286, 2021.

[3] D. Maloney, G. Freeman, and A. Robb, "It is complicated: Interacting with children in social virtual reality," in *2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*. IEEE, 2020, pp. 343–347.

[4] E. Deldari, D. Freed, J. Poveda, and Y. Yao, "An investigation of teenager experiences in social virtual reality from teenagers', parents', and bystanders' perspectives," in *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, 2023, pp. 1–17.

[5] D. Maloney, G. Freeman, and A. Robb, "A virtual space for all: Exploring children's experience in social virtual reality," in *Proceedings of the Annual Symposium on Computer-Human Interaction in Play*, 2020, pp. 472–483.

[6] D. Adams, A. Bah, C. Barwulor, N. Musaby, K. Pitkin, and E. M. Redmiles, "Ethics emerging: the story of privacy and security perceptions in virtual reality," in *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 2018, pp. 427–442.

[7] E. Dick, "Balancing user privacy and innovation in augmented and virtual reality," Information Technology and Innovation Foundation, Tech. Rep., 2021.

[8] P. Caserman, A. Garcia-Agundez, R. Konrad, S. Göbel, and R. Steinmetz, "Real-time body tracking in virtual reality using a vive tracker," *Virtual Reality*, vol. 23, pp. 155–168, 2019.

[9] V. Clay, P. König, and S. Koenig, "Eye tracking in virtual reality," *Journal of eye movement research*, vol. 12, no. 1, 2019.

[10] G. Kelly, "Kids deserve better privacy in virtual reality," Nov 2022. [Online]. Available: https://www.commonsensemedia.org/kids-action/articles/kids-deserve-better-privacy-in-virtual-reality

[11] N. Reed, "What are kids doing in the metaverse?" Mar 2022. [Online]. Available: https://www.commonsensemedia.org/kids-action/articles/what-are-kids-doing-in-the-metaverse

[12] A. Klein, "Common sense media says school vr tools violate privacy laws," Nov 2022. [Online]. Available: https://www.govtech.com/education/k-12/common-sense-media-says-school-vr-tools-violate-privacy-laws

[13] D. Maloney, S. Zamanifard, and G. Freeman, "Anonymity vs. familiarity: Self-disclosure and privacy in social virtual reality," in *Proceedings of the 26th ACM Symposium on Virtual Reality Software and Technology*, 2020, pp. 1–9.

[14] S. Sorensen, "Protecting children's right to privacy in the digital age: parents as trustees of children's rights," *Child. Legal Rts. J.*, vol. 36, p. 156, 2016.

[15] S. Livingstone, M. Stoilova, and R. Nandagiri, "Children's data and privacy online: growing up in a digital age: an evidence review," 2019.

[16] P. Kumar, S. M. Naik, U. R. Devkar, M. Chetty, T. L. Clegg, and J. Vitak, "'no telling passcodes out because they're private' understanding children's mental models of privacy and security online," *Proceedings of the ACM on Human-Computer Interaction*, vol. 1, no. CSCW, pp. 1–21, 2017.

[17] W. Shin, J. Huh, and R. J. Faber, "Tweens' online privacy risks and the role of parental mediation," *Journal of Broadcasting & Electronic Media*, vol. 56, no. 4, pp. 632–649, 2012.

[18] S. Chai, S. Bagchi-Sen, C. Morrell, H. R. Rao, and S. J. Upadhyaya, "Internet and online information privacy: An exploratory study of preteens and early teens," *IEEE Transactions on Professional Communication*, vol. 52, no. 2, pp. 167–182, 2009.

[19] D. Boyd and A. E. Marwick, "Social privacy in networked publics: Teens' attitudes, practices, and strategies," in *A decade in internet time: Symposium on the dynamics of the internet and society*, 2011.

[20] L. Zhang-Kennedy, C. Mekhail, Y. Abdelaziz, and S. Chiasson, "From nosy little brothers to stranger-danger: Children and parents' perception of mobile threats," in *Proceedings of the The 15th International Conference on Interaction Design and Children*, 2016, pp. 388–399.

[21] P. Wisniewski, H. Jia, H. Xu, M. B. Rosson, and J. M. Carroll, "" preventative" vs." reactive" how parental mediation influences teens' social media privacy behaviors," in *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing*, 2015, pp. 302–316.

[22] P. Wisniewski, A. K. Ghosh, H. Xu, M. B. Rosson, and J. M. Carroll, "Parental control vs. teen self-regulation: Is there a middle ground for mobile online safety?" in *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 2017, pp. 51–69.

[23] L. F. Cranor, A. L. Durity, A. Marsh, and B. Ur, "{Parents'} and {Teens'} perspectives on privacy in a {Technology-Filled} world," in *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, 2014, pp. 19–35.

[24] P. J. Wisniewski, H. Xu, M. B. Rosson, and J. M. Carroll, "Adolescent online safety: the" moral" of the story," in *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*, 2014, pp. 1258–1271.

[25] A. Hiniker, S. Y. Schoenebeck, and J. A. Kientz, "Not at the dinner table: Parents' and children's perspectives on family technology rules," in *Proceedings of the 19th ACM conference on computer-supported cooperative work & social computing*, 2016, pp. 1376–1389.

[26] M. Akter, L. Alghamdi, J. Kropczynski, H. R. Lipford, and P. J. Wisniewski, "It takes a village: A case for including extended family members in the joint oversight of family-based privacy and security for mobile smartphones," in *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, 2023, pp. 1–7.

[27] M. Akter, A. J. Godfrey, J. Kropczynski, H. R. Lipford, and P. J. Wisniewski, "From parental control to joint family oversight: Can parents and teens manage mobile online safety and privacy as equals?" *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. CSCW1, pp. 1–28, 2022.

[28] F. O'Brolcháin, T. Jacquemard, D. Monaghan, N. O'Connor, P. Novitzky, and B. Gordijn, "The convergence of virtual reality and social networks: threats to privacy and autonomy," *Science and engineering ethics*, vol. 22, pp. 1–29, 2016.

[29] B. Heller, "Reimagining reality: human rights and immersive technology," *Harvard Carr Center Discussion Paper Series*, 2020.

[30] A. Bar-Zeev, "The eyes are the prize: Eye-tracking technology is advertising's holy grail," *Retrieved April*, vol. 22, p. 2020, 2019.

[31] J. L. Kröger, O. H.-M. Lutz, and F. Müller, "What does your gaze reveal about you? on the privacy implications of eye tracking," *Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers 14*, pp. 226–241, 2020.

[32] N. Acosta, "Are ip addresses 'personal information'under ccpa?" *IAPP Privacy Advisor, April*, vol. 28, 2020.

[33] X. S. Initiative, "The xrsi privacy framework," 2020.

[34] K. Pearlman, X. Initiative, S. Visner, M. Magnano, and R. Cameron, "Securing the metaverse-virtual worlds need real governance," *Simulation Interoperability Standards Organization–SISO*, 2021.

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

[36] Q. Zheng, S. Xu, L. Wang, Y. Tang, R. C. Salvi, G. Freeman, and Y. Huang, "Understanding safety risks and safety design in social vr environments," *Proceedings of the ACM on Human-Computer Interaction*, vol. 7, no. CSCW1, pp. 1–37, 2023.

[37] P. Sykownik, D. Maloney, G. Freeman, and M. Masuch, "Something personal from the metaverse: goals, topics, and contextual factors of self-disclosure in commercial social vr," in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 2022, pp. 1–17.

[38] J. McVeigh-Schultz, A. Kolesnichenko, and K. Isbister, "Shaping pro-social interaction in vr: an emerging design framework," in *Proceedings of the 2019 CHI conference on human factors in computing systems*, 2019, pp. 1–12.

[39] J. McVeigh-Schultz, E. Márquez Segura, N. Merrill, and K. Isbister, "What's it mean to" be social" in vr? mapping the social vr design ecology," in *Proceedings of the 2018 ACM Conference Companion Publication on Designing Interactive Systems*, 2018, pp. 289–294.

[40] G. M. Garrido, V. Nair, and D. Song, "Sok: Data privacy in virtual reality," *arXiv preprint arXiv:2301.05940*, 2023.

[41] R. Trimananda, H. Le, H. Cui, J. T. Ho, A. Shuba, and A. Markopoulou, "{OVRseen}: Auditing network traffic and privacy policies in oculus {VR}," in *31st USENIX security symposium (USENIX security 22)*, 2022, pp. 3789–3806.

[42] D. Maloney, G. Freeman, and A. Robb, "Stay connected in an immersive world: Why teenagers engage in social virtual reality," in *Interaction Design and Children*, 2021, pp. 69–79.

[43] L. Blackwell, N. Ellison, N. Elliott-Deflo, and R. Schwartz, "Harassment in social vr: Implications for design," in *2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*. IEEE, 2019, pp. 854–855.

[44] K. Shriram and R. Schwartz, "All are welcome: Using vr ethnography to explore harassment behavior in immersive social virtual reality," in *2017 IEEE Virtual Reality (VR)*. IEEE, 2017, pp. 225–226.

[45] D. Maloney, G. Freeman, and D. Y. Wohn, "" talking without a voice" understanding non-verbal communication in social virtual reality," *Proceedings of the ACM on Human-Computer Interaction*, vol. 4, no. CSCW2, pp. 1–25, 2020.

[46] N. Sabri, B. Chen, A. Teoh, S. P. Dow, K. Vaccaro, and M. Elsherief, "Challenges of moderating social virtual reality," in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 2023, pp. 1–20.

[47] S. Youn, "Parental influence and teens' attitude toward online privacy protection," *Journal of Consumer Affairs*, vol. 42, no. 3, pp. 362–388, 2008.

[48] W. Shin and H. Kang, "Adolescents' privacy concerns and information disclosure online: The role of parents and the internet," *Computers in Human Behavior*, vol. 54, pp. 114–123, 2016.

[49] H. Nissenbaum, *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, 2020.

[50] P. Kumar, J. Vitak, M. Chetty, T. L. Clegg, J. Yang, B. McNally, and E. Bonsignore, "Co-designing online privacy-related games and stories with children," in *Proceedings of the 17th ACM conference on interaction design and children*, 2018, pp. 67–79.

[51] A. N. Joinson, C. B. Paine *et al.*, "Self-disclosure, privacy and the internet," *The Oxford handbook of Internet psychology*, vol. 2374252, pp. 237–252, 2007.

[52] N. C. Krämer and J. Schäwel, "Mastering the challenge of balancing self-disclosure and privacy in social media," *Current opinion in psychology*, vol. 31, pp. 67–71, 2020.

[53] C. Hallam and G. Zanella, "Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards," *Computers in Human Behavior*, vol. 68, pp. 217–227, 2017.

[54] H. Krasnova, E. Kolesnikova, and O. Guenther, "" it won't happen to me!": self-disclosure in online social networks," 2009.

[55] J. Nolan, K. Raynes-Goldie, and M. McBride, "The stranger danger: Exploring surveillance, autonomy, and privacy in children's use of social media." *Canadian Children*, vol. 36, no. 2, 2011.

[56] K. Subrahmanyam, R. E. Kraut, P. M. Greenfield, and E. F. Gross, "The impact of home computer use on children's activities and development," *The future of children*, pp. 123–144, 2000.

[57] S. Livingstone, J. Davidson, J. Bryce, S. Batool, C. Haughton, and A. Nandi, "Children's online activities, risks and safety: a literature review by the ukccis evidence group," 2017.

[58] S. Livingstone and P. K. Smith, "Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age," *Journal of child psychology and psychiatry*, vol. 55, no. 6, pp. 635–654, 2014.

[59] L. Palen and P. Dourish, "Unpacking" privacy" for a networked world," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, 2003, pp. 129–136.

[60] S. Livingstone, "Children's privacy online: experimenting with boundaries within and beyond the family," 2006.

[61] H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: an interdisciplinary review," *MIS quarterly*, pp. 989–1015, 2011.

[62] K. Sun, C. Sugatan, T. Afnan, H. Simon, S. A. Gelman, J. Radesky, and F. Schaub, ""they see you're a girl if you pick a pink robot with a skirt": A qualitative study of how children conceptualize data processing and digital privacy risks," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–34.

[63] B. Shmueli and A. Blecher-Prigat, "Privacy for children," *Colum. Hum. Rts. L. Rev.*, vol. 42, p. 759, 2010.

[64] S. Livingstone, "Developing social media literacy: How children learn to interpret risky opportunities on social network sites," *Communications*, vol. 39, no. 3, pp. 283–303, 2014.

[65] J. C. Yip, K. Sobel, X. Gao, A. M. Hishikawa, A. Lim, L. Meng, R. F. Ofiana, J. Park, and A. Hiniker, "Laughing is scary, but farting is cute: A conceptual model of children's perspectives of creepy technologies," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–15.

[66] Y. Feng and W. Xie, "Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors," *Computers in Human Behavior*, vol. 33, pp. 153–162, 2014.

[67] A. Bowyer, K. Montague, S. Wheater, R. McGovern, R. Lingam, and M. Balaam, "Understanding the family perspective on the storage, sharing and handling of family civic data," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–13.

[68] A. Duerager and S. Livingstone, "How can parents support children's internet safety?" 2012.

[69] M. Madden, S. Cortesi, U. Gasser, A. Lenhart, and M. Duggan, "Parents, teens, and online privacy." *Pew internet & American life project*, 2012.

[70] P. Wisniewski, H. Xu, M. B. Rosson, and J. M. Carroll, "Parents just don't understand: Why teens don't talk to parents about their online risk experiences," in *Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing*, 2017, pp. 523–540.

[71] L. Blackwell, E. Gardiner, and S. Schoenebeck, "Managing expectations: Technology tensions among parents and teens," in *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, 2016, pp. 1390–1401.

[72] S. T. Hawk, L. Keijsers, W. W. Hale III, and W. Meeus, "Mind your own business! longitudinal relations between perceived privacy invasion and adolescent-parent conflict." *Journal of Family Psychology*, vol. 23, no. 4, p. 511, 2009.

[73] S. Livingstone and M. Bober, "Regulating the internet at home: contrasting the perspectives of children and parents," in *Digital generations*. Routledge, 2013, pp. 93–113.

[74] J. G. Smetana, ""it's 10 o'clock: Do you know where your children are?" recent advances in understanding parental monitoring and adolescents' information management," *Child Development Perspectives*, vol. 2, no. 1, pp. 19–25, 2008.

[75] B. Teitell, "In digital world, kids gain the upper hand," *Boston Globe, September*, vol. 5, 2013.

[76] M. A. A. Majid, M. Othman, S. F. Mohamad, S. A. H. Lim, A. Yusof *et al.*, "Piloting for interviews in qualitative research: Operationalization and lessons learnt," *International Journal of Academic Research in Business and Social Sciences*, vol. 7, no. 4, pp. 1073–1080, 2017.

[77] R. Jääskeläinen, "Think-aloud protocol," *Handbook of translation studies*, vol. 1, pp. 371–374, 2010.

[78] [Online]. Available: https://www.qualtrics.com/

[79] J. Saldaña, *The coding manual for qualitative researchers*. sage, 2021.

[80] D. Wermke, N. Wöhler, J. H. Klemmer, M. Fourné, Y. Acar, and S. Fahl, "Committed to trust: A qualitative study on security & trust in open source software projects," in *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022, pp. 1880–1896.

[81] L. Gröber, R. Mrowczynski, N. Vijay, D. A. Muller, A. Dabrowski, and K. Krombholz, "To cloud or not to cloud: A qualitative study on {Self-Hosters}'motivation, operation, and security mindset," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 2491–2508.

[82] S. Höltervennhoff, P. Klostermeyer, N. Wöhler, Y. Acar, and S. Fahl, "{"I} wouldn't want my unsafe code to run my {pacemaker"}: An interview study on the use, comprehension, and perceived risks of unsafe rust," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 2509–2525.

[83] N. McDonald, S. Schoenebeck, and A. Forte, "Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice," *Proceedings of the ACM on human-computer interaction*, vol. 3, no. CSCW, pp. 1–23, 2019.

[84] B. Saunders, J. Sim, T. Kingstone, S. Baker, J. Waterfield, B. Bart-lam, H. Burroughs, and C. Jinks, "Saturation in qualitative research: exploring its conceptualization and operationalization," *Quality & quantity*, vol. 52, pp. 1893–1907, 2018.

[85] J. J. Francis, M. Johnston, C. Robertson, L. Glidewell, V. Entwistle, M. P. Eccles, and J. M. Grimshaw, "What is an adequate sample size? operationalising data saturation for theory-based interview studies," *Psychology and health*, vol. 25, no. 10, pp. 1229–1245, 2010.

[86] S. Steinberg, "Parent's guide to vr headsets and vr games for kids," Jun 2023. [Online]. Available: https://www.verizon.com/about/parenting/parents-guide-vr-headsets-and-vr-games-kids

[87] E. Gent and LiveScience, "Are virtual reality head-sets safe for children?" Dec 2016. [Online]. Available: https://www.scientificamerican.com/article/are-virtual-reality-headsets-safe-for-children/

[88] M. Jay, "What parents need to know about vr," Apr 2023. [Online]. Available: https://www.esrb.org/blog/what-parents-need-to-know-about-vr/

[89] P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. F. Cranor, "Ex-ploring how privacy and security factor into iot device purchase behavior," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–12.

[90] S. Baker, J. Waycott, R. Carrasco, R. M. Kelly, A. J. Jones, J. Lilley, B. Dow, F. Batchelor, T. Hoang, and F. Vetere, "Avatar-mediated communication in social vr: an in-depth exploration of older adult interaction in an emerging communication platform," in *Proceedings of the 2021 CHI conference on human factors in computing systems*, 2021, pp. 1–13.

[91] K. Fu, Y. Chen, J. Cao, X. Tong, and R. LC, "" i am a mirror dweller": Probing the unique strategies users take to communicate in the context of mirrors in social virtual reality," in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 2023, pp. 1–19.

[92] S. Barth and M. D. De Jong, "The privacy paradox–investigating discrepancies between expressed privacy concerns and actual online behavior–a systematic literature review," *Telematics and informatics*, vol. 34, no. 7, pp. 1038–1058, 2017.

[93] P. Wisniewski, "The privacy paradox of adolescent online safety: A matter of risk prevention or risk resilience?" *IEEE Security & Privacy*, vol. 16, no. 2, pp. 86–90, 2018.

[94] S. Yardi and A. Bruckman, "Social and technical challenges in parenting teens' social media use," in *Proceedings of the SIGCHI conference on human factors in computing systems*, 2011, pp. 3237–3246.

[95] M. Mazmanian and S. Lanette, "" okay, one more episode" an ethnography of parenting in the digital age," in *Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing*, 2017, pp. 2273–2286.

[96] A. Ekambaranathan, J. Zhao, and M. Van Kleek, "Understanding value and design choices made by android family app developers," in *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–10.

[97] A. Ekambaranathan, J. Zhao, and M. Van Kleek, ""money makes the world go around": Identifying barriers to better privacy in children's apps from developers' perspectives," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–15.

[98] A. Ekambaranathan, J. Zhao, and M. Van Kleek, "How can we design privacy-friendly apps for children? using a research through design process to understand developers' needs and challenges," *Proceedings of the ACM on Human-Computer Interaction*, vol. 7, no. CSCW2, pp. 1–29, 2023.

[99] A. K. Ghosh, K. Badillo-Urquiola, S. Guha, J. J. LaViola Jr, and P. J. Wisniewski, "Safety vs. surveillance: what children have to say about mobile apps for parental control," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–14.

[100] J. Li, K. Sun, B. S. Huff, A. M. Bierley, Y. Kim, F. Schaub, and K. Fawaz, ""it's up to the consumer to be smart": Understanding the security and privacy attitudes of smart home users on reddit," in *IEEE Symposium on Security and Privacy (SP)(SP)*. IEEE Computer Society Los Alamitos, CA, 2023, pp. 380–396.

[101] J. Holvast, "History of privacy," in *The history of information security*. Elsevier, 2007, pp. 737–769.

[102] N. Malazizi, H. Alipour, and H. Olya, "Risk perceptions of airbnb hosts: Evidence from a mediterranean island," *Sustainability*, vol. 10, no. 5, p. 1349, 2018.

[103] P. M. Regan, "Privacy as a common good in the digital world," *Information, Communication & Society*, vol. 5, no. 3, pp. 382–405, 2002.

[104] P. Emami-Naeini, Y. Agarwal, L. F. Cranor, and H. Hibshi, "Ask the experts: What should be on an iot privacy and security label?" in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 447–464.

[105] P. Emami-Naeini, J. Dheenadhayalan, Y. Agarwal, and L. F. Cranor, "Which privacy and security attributes most impact consumers' risk perception and willingness to purchase iot devices?" in *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 519–536.

[106] M. Wolfe, "Childhood and privacy. altman, i. and wohmill, jf children and the environment," 1978.

[107] E. A.-L. Lee and K. W. Wong, "A review of using virtual reality for learning," *Transactions on edutainment I*, pp. 231–241, 2008.

[108] S. Helsel, "Virtual reality and education," *Educational Technology*, vol. 32, no. 5, pp. 38–42, 1992.

[109] V. S. Pantelidis, "Virtual reality in the classroom," *Educational technology*, vol. 33, no. 4, pp. 23–27, 1993.

[110] T. Kojić, D. Ali, R. Greinacher, S. Möller, and J.-N. Voigt-Antons, "User experience of reading in virtual reality—finding values for text distance, size and contrast," in *2020 Twelfth International Conference on Quality of Multimedia Experience (QoMEX)*. IEEE, 2020, pp. 1–6.

Appendix A.
Usage and Demographic Tables

TABLE 2. PARENTS' AND CHILDREN'S VR USAGE.

ID	VR Device Ownership	Parent's VR Usage	Children's VR usage.
P1	Meta Quest Pro	Creativity, Education, Gaming, Health, Productivity, Socialization, Streaming	Unspecified
P2	Meta	Gaming, Work	No longer interested
P3	Meta Quest 2	Gaming, Exploration of VR	Gaming
P4	Oculus	Creativity, Education, Gaming, Productivity, Socialization	Creativity, Education, Gaming
P5	Meta Quest 2	Gaming, Health, Socialization, Streaming	Gaming
P6	Meta Quest 2	Creativity, Gaming, Socialization	No longer interested
P7	Meta Quest	Gaming	Gaming
P8	Meta Oculus Quest 2	Creativity, Education, Gaming, Health, Streaming	Creativity, Education, Gaming, Socialization
P9	DEVASCO & Bnext	Creativity, Education, Health, Virtual Tours	Creativity, Education, Health, Virtual Tours
P10	Oculus, Google Cardboard	Education	Education, Gaming
P11	Oculus, Microsoft Hololens	Creativity, Education, Gaming, Productivity, Work	Gaming
P12	Oculus	Creativity, Gaming, Socialization, Streaming	Unspecified
P13	Oculus	Gaming, Health	Gaming, Health
P14	Oculus Meta Quest	Gaming	Gaming
P15	Oculus	Gaming, Socialization	Gaming, Socialization
P16	Oculus Quest 2	Education, Streaming	Gaming
P17	Meta Oculus	Education, Streaming	Gaming, Streaming
P18	Oculus	Gaming	Gaming
P19	Oculus Quest 2	Education, Gaming, Health, Socialization, Streaming	Gaming
P20	Oculus	Creativity, Gaming, Socialization, Streaming	Gaming

TABLE 3. PARENTS' AGE, GENDER, RACE, EDUCATION BACKGROUND, AND RECRUITMENT CHANNEL DISTRIBUTIONS.

Age		Gender		Race		Education Background		Recruitment Channel	
25-34	10%	M	70%	White	55%	Doctorate degree	5%	Personal connections	5%
35-44	15%	F	30%	Black	20%	Master's degree	45%	LinkedIn	10%
45-54	65%			Asian	20%	Professional degree	5%	Facebook	10%
55-64	10%			Prefer not to say	5%	Bachelor's degree	30%	Discord	10%
						Associate's degree	5%	Reddit	5%
						1 or more years of college credit, no degree	5%	School Advertisement	60%
						Regular high school diploma	5%		

Appendix B.
Study Artifacts

The pre-screening survey, interview protocol, live survey, and final codebook are available at:
https://osf.io/4p9c3/?view_only=b1dfae593e5142a6ac0bb59866479d40.

Appendix C.
Meta-Review

The following meta-review was prepared by the program committee for the 2024 IEEE Symposium on Security and Privacy (S&P) as part of the review process as detailed in the call for papers.

C.1. Summary

This paper investigates parents' perceptions of security and privacy risks their children face in VR. The authors conduct 20 interviews with parents of children who have used VR to find perceptions of risks, mitigation strategies, and expectations from stakeholders. They find that parents are generally unaware of potential risks, have various protective practices (including active strategies), and request a variety of security & privacy measures. An extensive discussion of their findings in the context of prior work is included.

C.2. Scientific Contributions

- Provides a Valuable Step Forward in an Established Field

C.3. Reasons for Acceptance

1) This paper investigates an important and timely research problem
2) The selection of methods is appropriate and the study is well executed.
3) The authors present interesting findings and an actionable recommendation section.

C.4. Noteworthy Concerns

1) Though there is a discussion, the VR threats found in this work aren't strongly tied to VR threats uncovered in prior work.

Appendix D.
Response to the Meta-Review

When appropriate, we mapped the VR threats in our findings to a previous study as an example [40] (e.g., Sections 4.1.2 & 5), calling for raising parents' risk awareness of VR server adversaries. Due to our focus on empirical contributions, we encourage future work to have more in-depth theoretical discussions, mapping the identified VR threats to well-established threat models.