YOUTH DIGITAL SAFETY EXPERIENCES IN DIFFERENT SOCIOTECHNICAL ENVIRONMENTS AND SPACES

A Dissertation

Presented to the Faculty of the Graduate School

of Cornell University

in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

by

Diana Freed

August 2023

YOUTH DIGITAL SAFETY EXPERIENCES IN DIFFERENT SOCIOTECHNICAL ENVIRONMENTS AND SPACES

Diana Freed, Ph.D.

Cornell University 2023

Digital technologies, such as mobile devices, social virtual reality, and social networks, play an increasingly significant role in both posing risks and creating opportunities for youth. In this dissertation, Study 1 contributes to a relational understanding of the digital-safety landscape faced by youth around digitally-mediated attacks, adding nuance, complexity, and comprehensiveness to prior work that are important to consider in research, design, and policy efforts to support the digital safety of youth. This study broadens the understanding of digital threats by providing a nuanced image of attackers and threats. Study 2 investigates teenagers' experiences with harassment in social virtual reality (social VR) from the perspectives teenagers, parents, and bystanders. This research contributes to the literature by identifying new forms of harassment in social VR. This research is also the first study to take a multi-stakeholder perspective in VR and highlights the discrepancies among these three groups regarding their perceptions and responses to these threats. Study 3 explores the help-seeking behavior of youth in response to digital harms and threats. It describe the support systems that youth engage with, and how their help-seeking behaviors differ based on the digital threats they encounter, actual or anticipated risks, and the severity and persistence of risks. Together these chapters illuminate the multidimensional landscape of youth digital abuse, examining its complexities from various perspectives.

BIOGRAPHICAL SKETCH

Diana Freed received her BA from CUNY Hunter College, graduating magna cum laude. She then furthered her education receiving master's degrees from New York University and Columbia University. She has pursued her PhD in Information Science at Cornell University. She is a recipient of an Engaged Cornell Graduate Student Grant, a Meta Research Doctoral Fellowship, a Digital Life Doctoral Fellowship, and a Data and Society Research Institute Fellowship. Her research primarily focuses on improving online safety and well-being for vulnerable and marginalized populations, leveraging tools from various fields such as human-computer interaction, computer security, privacy, inclusive design, behavioral health, and public policy.

To my family and friends

ACKNOWLEDGEMENTS

Throughout this journey, I have been fortunate to have had the support, guidance, and friendship of many individuals, and I want to express my appreciation. First to my Chair, Dr. Natalie Bazarova, you have been an unwavering beacon of guidance and inspiration. I am extremely grateful for your time, support, and encouragement. Your wisdom and profound expertise have not only inspired me but have immensely propelled my work forward. Your mentorship has illuminated the path throughout my graduate journey and made this a wonderful experience. I am fortunate to have you as my Chair and I have learned so much from you. Next, I'd like to express my heartfelt gratitude to Dr. Dan Cosley. Thank you for your consistent support and your continual encouragement throughout my academic journey. Thank you for all the time you took to talk me through my ideas and encourage me. I greatly appreciate your kindness and dedication. I would also like to express my deepest appreciation to Dr. Tanzeem Choudhury. I greatly appreciate and value your continuous support and guidance, your unique ability to understand and empathize, and the profound impact you have had on me. You have taught me so much and I am extremely grateful for your mentorship. To Dr. Karen Levy, I am so fortunate to have you as a mentor. I am grateful to have the opportunity to learn from your scholarship. Your unwavering support, friendship, and insightful guidance have been invaluable. In addition to my committee members, a special thank you to Dr. Deborah Estrin for your extraordinary mentorship and support for which I am forever grateful. Additionally, I would like to thank my collaborators, the Social Media Lab and my cohort. Finally, to my family and friends, thank you for everything!

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 1

INTRODUCTION AND THEORETICAL OVERVIEW

1.1 Digital Technologies and Youth: Opportunities and Concerns

The continual integration of technology into the lives of youth has presented many opportunities for youth but has also raised concerns about their digital safety. Digital technologies, such as mobile devices, Internet of Things (IoT) devices, social virtual reality, and social networks, provide youth with the opportunity to connect with friends, develop relationships, engage with online communities, and build supportive relationships. In addition, adolescence (12-18 yrs of age) is a time when youth are exploring their identity, testing boundaries, and establishing autonomy [71, 72]. For youth living in communities characterized by risks related to, for example, health, violence, or discrimination, digital media creates opportunities to find social support and advocacy and to discover resources that foster resilience [162].

Digital spaces, particularly social media, act as an exploratory space for youth to investigate their identity and form relationships [39, 38]. Youth can express themselves on social media through multiple accounts and platforms allowing for a broad range of self-expression based on the features and tools available (e.g., photos, video, text) [38]. The emergence of social VR adds a new dimension to digital interaction. Unlike traditional online spaces that rely primarily on text messages and static avatars for interaction, social VR offers a more immersive, multi-user environment. It allows for a heightened sense of presence through

features like real-time body movement tracking, synchronous voice communication, and simulated tactile interactions. These novel characteristics introduce new dynamics into relationship building, fostering a unique interactive experience [149, 150, 147]. Given all of these complexities, ensuring the safety and well-being of youth is of paramount importance.

According to Pew Research, an estimated 95% of U.S. youth between the ages of 12 and 17 have access to a smartphone, and 45% report having regular access to devices [129]. Consistent access and exposure to media, including content posted by peers, has raised concerns regarding increased exposure to inappropriate content, online harassment, sexual coercion, and cyberbullying [15, 174, 112, 145]. Unfettered access to digital technologies may enable youth to engage with risky sexual content, as well as with adults that intend to manipulate youth for the purpose of sexual exploitation or "grooming" [223]. Social VR exacerbates risks for youth as they explore virtual spaces and enter into adult environments. However, as these interactions take place in a virtual environment, the cues used to form judgments and impressions of strangers may be different than those in traditional online social spaces. Social VR platforms introduce new technology characteristics and user experiences, which may lead to harassment and sexual abuse. At-risk populations face greater risks and consequences of privacy invasions and security failures.

1.1.1 Youth as "at-risk users"

Digital threats broadly affect everyone online, however youth, in particular, are at risk due to their risk-seeking behavior and their limited understanding of

potential digital threats. As a result, special care has to be invested to understand the sociotechnical complexities that impact their exposure to digital risks as well as their privacy and security practices and ability to navigate evolving technologies.

Youth are often labeled as "at-risk users" [239], and may struggle with accurately assessing the online risks they face, thereby possibly failing to provide adequate protection for themselves. According to the risk-centric framework by Jia et al. [109], youth learn risk-coping behaviors through digital risk-taking, thereby exposing themselves to risky situations and possible risk escalation. This dynamic is different from adults, whose online risk-taking behaviors are shaped more by cognitive concerns than by experiential learning. Youth risk-taking is important to account for in digital spaces as youth seek heightened stimulation and have an underdeveloped self-regulatory system [212].

While prior research has highlighted the multifaceted nature of adolescent online risk-exposure, there is still a considerable gap in the literature regarding how these risks interact with the unique vulnerabilities of different youth populations in various environments in response to different threats. Scholars have recognized the importance of exploring adolescent online risk-exposure in an effort to explore effective ways to keep youth safe online [19, 36, 93, 241, 198, 244, 77, 242]. Research approaches have included studies that focus on discourse surveys revealing the importance of parental trust, control, or involvement [93] as well as design strategies for parental mediation of adolescent smartphone use [117].

Additional research has included classifications of digital risks experienced by youth distinguishing between non-sexual and sexual risks [137, 135], with further distinctions by the nature of risks, types of content, and activities on-

line [22, 21]. This work has included a classification of online risk for youth into 4 categories: content risks, contact risks, conduct risks, and contract risks [211, 138, 130]. More recent work has started to call out the interrelated nature of risks, with exposure to one digital risk (e.g., sexting) predicting a youth's engagement with other types of digital risks (e.g., risks of sexual solicitations) [213]. These risks and threats experienced by youth can be amplified by existing real world vulnerabilities [138, 173], including unstable living situations, foster care, introversion, mental health issues, witnessing or experiencing prior trauma, disabilities, and immigrant or refugee status [207, 181, 131]. Prior work has also explored digital risks experienced by LGBTQ youth [96, 59] as well as how safe spaces can become places where harmful interactions occur for transgender and gender non-conforming people [203].

There is also a limited understanding of how youth utilize social media as a vehicle to find support [90]. Scholars have described how youth use Facebook to find social support and several studies have explored how youth seek support via publicly accessible content tied to topics focusing on sexual experiences [189, 94, 106]. Other work explored Instagram Direct Messages for peer support among youth in the context of mental health and personal issues [106]. The investigation of help-seeking behaviors and resources for seeking help has predominantly occurred within the realm of mental health support [139], and amidst cases of cyber-harassment victimization [180].

Considering the range of circumstances in which digital abuse occurs, it is important to understand how youth engage with these platforms as well as how the features within the applications provide protection or are misused in abuse contexts. My dissertation research collectively advances the understanding

of digital safety experiences of youth and how they navigate and respond to digital threats and attacks within a broad support system. The studies in this dissertation explore youth digital safety experiences in different sociotechnical environments and spaces that encompass help-seeking behavior in response to digital risks and attacks as well as the role of stakeholders within these contexts. Chapters 2 and 3 investigate the multidimensional landscape of digital abuse by outlining the types of risks and harms youth encounter in digital spaces, the types of attackers and relationships within which abuse takes place, and the digital contexts in which abuse occurs. They provide a comprehensive examination of how different stakeholders conceptualized and managed risk, as well as the shortcomings of both the technology and support systems designed to protect youth. Additionally, to develop prevention and intervention strategies, there is a need to distill how youth seek help in response to these digital threats and attacks. Chapter 4 presents the analysis of the help seeking behavior of youth and pathways used in response to digital abuse experiences. Together, they present an in-depth investigation of the multifaceted issue of digital abuse faced by youth, uncovering the risks and threats they encounter, the means by which they seek help, and the roles of various stakeholders in this digital safety landscape, with the ultimate goal of informing more effective prevention and intervention strategies.

1.2 The State of Support in Help-Seeking

Despite a burgeoning research interest to youth digital safety [214, 244, 190, 18, 5], there has been a limited understanding of the digital threats and harms youth experience from a multi-stakeholder perspective. As discussed in Chapter 2

and Chapter 4, parents, guardians and caregivers are important yet overlooked groups in helping to teach youth how to responsibly and safely navigate the online world while also serving as crucial coordinators if children are subject to harmful activity. Prior work has discussed the digital divide, revealing how disparities in technology access and literacy can influence family communication dynamics across generational lines [28]. We expand upon this work in Chapter 2 discussing how the efficacy of protective practices may be impacted by parental digital literacy as they may implement a protective practice based on an assumed understanding rather than having the technology knowledge to directly address the threat. Relatedly, in Chapter 2 we describe how adults self-reported challenges in understanding the applications used by youth impacting their ability to mitigate digital threats and implement effective protective practices.

1.3 Understanding Digital Safety Through a Social and Ecological Lens

Throughout this research we discuss digital threats and support provisions in terms of a broader ecosystem or landscape recognizing that youth engage with a broad range of stakeholders. These complex factors influencing the digital safety of youth can be viewed through the lens of a socio-ecological model, which recognizes multiple layers of influence on individuals' behaviors, spanning the micro to the macro-level of society [43]. The socio-ecological model is a conceptual model introduced by Urie Bronfrenbrenner to understand human development [42]. This model has been adapted and applied to various contexts including youth violence [227], child abuse [83], and resilience [229] and puts

forth the idea that our behaviors and experiences are shaped by a multitude of interconnected factors.

According to the socio-ecological model, youth are embedded within various ecosystems—family, peers, schools, community, and larger societal structures—and their behavior is shaped by the dynamic interactions within and across these ecosystems. This includes their online behavior and how they perceive, engage with, and mitigate digital risks.

Theories that take a social and ecological lens are useful for better understanding youth safety. In this context, digital safety is not just an individual concern but a socio-ecological issue, where multiple ecosystems of influence need to be considered in holistic risk assessment and management strategies. From this perspective, strategies for managing online risks should involve all the stakeholders in youth's ecosystems and take into account the online-offline convergence in youth's lives. The socio-ecological model helps to highlight the importance of comprehensive and coordinated efforts at different levels to ensure youth's digital safety. This dissertation investigates youth digital safety in the context of understanding both the abuse and the safety experiences of youth as happening within these ecosystems. For example, Chapter 2 identifies the stakeholders within the ecosystems and how they provide support, the protective practices used, and the encounters with youth in conjunction with other stakeholders to support youth in mitigating abuse experiences. Chapter 3 is the first social virtual reality study to provide multi-stakeholder perspectives including teenagers, bystanders, and parents in response to youth experiences with abuse in social VR. In Chapter 4 we further explore the help-seeking behavior of youth, identifying help-seeking pathways in response to digital threats and attacks and

examine how youth engage with stakeholders and technology directly in the face of these digital risks and harms.

The socio-ecological model also underscores the need for a deeper understanding of the digital threats and harms that youth experience within the broader social context. It highlights the crucial role of adults—not just parents and caregivers but also educators, policymakers, and the community at large—in shaping the digital ecosystem of youth and influencing their ability to navigate online risks. Therefore, efforts to bridge the digital divide among adults and to strengthen their capacity to guide and support youth in the digital world become essential. In Chapter 4 we describe the obstacles to youth help-seeking that arise as a result of both youths' perception of adults' understanding of technology as well as the importance of a shared terminology around digital threats and harms. Here we highlight the importance of facilitating conversations around digital abuse prevention and mitigation.

The socio-ecological model informs our research and calls for a shift from a narrow focus on individual behaviors to a broader systemic view that considers the multifaceted and interrelated factors that influence youth's online experiences and ability to cope with digital risks within a support system. This can lead to more comprehensive and contextualized strategies to foster a safer and more supportive digital environment for youth.

1.4 Contribution and Organization of Dissertation Chapters

The structure of this dissertation is organized in the following way. Chapter 2 (Study 1) contributes to a relational understanding of the digital-safety landscape

faced by youth around digitally-mediated attacks, adding nuance, complexity, and comprehensiveness to prior work that are important to consider in research, design, and policy efforts to support the digital safety of youth. We conducted a qualitative study using semi-structured interviews and focus group discussions for data collection conducted with 36 youth (ages 10 - 17) and 65 adult stakeholders from 13 states. Interviews focused on harms, attackers, and attacks youth face, along with shortcomings of both the technology and protective practices used by stakeholders to protect youth. Youth in this study came from different backgrounds and had different experiences with digitally mediated attacks and harms. This included youth who had experienced or witnessed domestic and or sexual violence, youth who participated in healthy relationship programs and youth who were not receiving support from any social service agencies or participated in school organized prevention or intervention programs. Through interviews with adults and youth we identified the stakeholders in the digital safety landscape to include parents, guardians, peers, educators, lawyers, advocates, and law enforcement.

This study expands the current understanding of digital threats that associates particular threats with specific attackers (e.g., cyberbullying with peers) [177, 63]. First, it broadens the understanding of digital threats by providing a nuanced image of attackers and threats. Additionally we highlight the importance of youth agency and co-design with youth in the development of security and privacy design noting that the protective practices adults implement are perceived by youth as intrusive and/or limiting their autonomy. This research fills a gap in the HCI literature identified in a recent review of youth risks and harms online [213] by providing a comprehensive picture that maps the various threats, attackers, and contexts in which they occur, the pathways between dif-

ferent threats, and protective practices employed by youth and the adults who support them.

Chapter 3 (Study 2) is a qualitative study using semi-structured interviews for data collection that investigates teenagers' (13-17 yrs of age) experiences with harassment in social virtual reality (social VR) from the perspectives of 8 teenagers, 7 parents, and 9 bystanders. This research contributes to the literature by identifying new forms of harassment in social VR such as *erotic role play* (ERP), a type of role-playing activity in which users adorn their avatars with components that have sexual connotations) and abuse through *phantom sense*, a phenomenon caused by immersion in a VR environment where a user's brain tricks their physical body into experiencing the touch sensations happening to their virtual body in virtual environments. In terms of ERP, many teenager participants normalized these activities and did not consider participation in this behavior as posing a threat to their safety. Throughout this study there conflicting perceptions of safety mainly stemming from teenagers perceptions of social norms which included engaging with strangers to adult perceptions of the behavior as threat to safety. This research is also the first study to take a multi-stakeholder perspective in VR and highlights the discrepancies among these three groups regarding their perceptions and responses to these threats. These complementary perspectives uncover nuances around teenagers' threats and point at opportunities for designing safety features and ensuring a safer virtual environment for youth.

Study 3 (Chapter 4) draws on semi-structured interviews and focus group discussion with 101 stakeholders in which we re-analyzed the data-set from Study 1 (Chapter 2, Study 1 section 2.3) to identify help-seeking behaviors.

This paper explores the help-seeking behavior of youth in response to digital harms and threats. We describe the support systems that youth engage with, and how their help-seeking behaviors differ based on the digital threats they encounter, actual or anticipated risks, and the severity and persistence of risks. Additionally, we explore how security reporting tools align with help-seeking needs of youth and the threats that they encounter, and how risk behavior and protective practices in their immediate environment contribute to their willingness to engage with support systems. We also expand the boundaries of the ecological support [233] and communal coping [143] models to accommodate digital abuse situations and offer new perspectives regarding the needs and goals of individuals in digital abuse situations.

Additionally, building upon an ecological support approach [143] and a communal coping model [233], we propose an analytical framework for digital help-seeking that expands upon prior conceptual model [193]. This accounts for an overall help-seeking ecosystem, rather than help-seeking on a single platform or from a particular support source, in order to untangle the social and contextual dynamics of help-seeking behaviors, the dynamic interplay of different support resources, and their relationship to different types of digital risks and harms.

This study (Chapter 4) contributes to a growing body of research dedicated to understanding the complexities of the digital-safety landscape [180, 213] and challenges of help-seeking [46, 106], as well as research promoting youth well-being through help-seeking, resilience, and digital safety interventions [5, 128, 52, 61]. Understanding youth help-seeking behaviors in response to digital threats requires acknowledging that there is no singular or linear pathway. Instead, help-seeking is a multifaceted process, influenced by various factors and channeled

through multiple pathways that could be activated concurrently or sequentially. For instance, a youth could turn to self-education, while also engaging peers, family, or tech company security and privacy features or engaging moderators in their journey to address digital abuse. This study is the first study to explore youth digital help-seeking from a multi-stakeholder perspective.

Finally, Chapter 5 provides a general discussion of these empirical findings and highlights opportunities for future research. My future research will continue to address security, privacy, and safety challenges of societal importance, with an emphasis on designing and developing solutions that enhance protection for vulnerable and marginalized populations.

Together these chapters illuminate the vast and multidimensional landscape of youth digital abuse, examining its complexities from various perspectives - the different types of digital risks and harms, distinct threat models, the diversity of attackers, and the intricate relationships within which abuse takes place. This research underscores the cross-context vulnerabilities highlighting how attacks move across multiple accounts, platforms, and into real-world interactions. The exploration extends to platform features and their potential risks for vulnerable youth, recognizing the disparity in expectations and understanding between youth and adult stakeholders.

Additionally, this work encompasses interactions in social VR, where unique challenges emerge. We investigate teenagers' safety concerns in social VR, providing insights into novel forms of harassment and sexual abuse within this realm. We propose design guidelines that can mitigate risks and support the safety and well-being of teenagers in these digital spaces and provide privacy and security considerations when designing technology for vulnerable youth,

highlighting the need for a more inclusive and safer digital environment.

Through this research we advance the current understanding of youth digital safety that can inform the development and deployment of intervention and prevention tools (e.g., technological innovations, policy changes, and education) to help improve youth digital safety and well-being.

Related publications. These thesis contributions have directly extended the body of research relating to the digital risks and harms within the context of the youth digital-safety ecosystem. I have shared these findings with a wider academic audience via conference presentations and publications in archival proceedings. The work within this thesis has been accepted and presented at peer-reviewed conferences:

1. Freed, Diana, Natalie N. Bazarova, Sunny Consolvo, Eunice J. Han, Patrick Gage Kelley, Kurt Thomas, and Dan Cosley. "Understanding Digital-Safety Experiences of Youth in the US." In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, pp. 1-15. 2023. (Study 1)

2. Deldari, Elmira*, Diana Freed*, Julio Poveda, and Yaxing Yao. "An Investigation of Teenager Harassment in Social Virtual Reality from Teenagers', Parents', and Bystanders' Perspectives." SOUPS, 2023. *contributed equally (Study 2)

CHAPTER 2

UNDERSTANDING DIGITAL-SAFETY EXPERIENCES OF YOUTH IN THE U.S.

2.1 Introduction

The increasing integration of technology into the daily lives of youth[1] has raised concerns about their digital safety. The landscape of digitally-mediated threats youth might experience is quite broad; it includes cyberbullying and harassment [118, 20, 15], sexual violence [17, 67], dangerous challenges [120, 114], misinformation [225], fraud [105], exposure to dangerous posts and groups [127], and more. The press often raises awareness of threats through attention-grabbing cases like catfishing [218] or sexual predation [166]. While such incidents can be tragic, these highly visible, viral narratives about threats may obscure the much wider range of less sensational risks youth often encounter online.

Prior work has explored youth experiences with physical, sexual, and emotional threats. This includes work on bullying and trafficking that predate widespread online access [108, 172, 49], and more recent studies addressing how technology may exacerbate these harms [244, 189, 165, 134]. These studies often focused on a particular harm or threat, or how a novel technology is misused. This type of focus offers deep insights into the risks youth face in particular cases, but leaves the HCI community without a comprehensive perspective on the myriad of threats faced by youth today. Others have called for research that moves toward more comprehensive perspectives, calling for work that maps the various threats, attackers, and contexts in which they occur; the pathways

[1] For the purposes of this chapter, we define *youth* as people aged 10–17.

between different threats; and protective practices employed by youth and the adults who support them within the protective ecosystem [213]. Further, although youth online behavior is often studied through secondary analysis of online trace data [95, 94, 116, 189], and youth themselves are sometimes involved through survey [111] and diary methods [244, 8], on balance, youth voices are underrepresented in academic literature regarding digitally-mediated threats [47].

In this paper, we seek to narrow these gaps around including youth voices and providing more comprehensive views of digital risks and protective practices through a qualitative study with 36 youth and 65 adults who support youth. The adults included parents, teachers, and social service advocates, while the youth spanned a wide spectrum, including many who have experienced or witnessed prior abuse—a group that is often not included in discussions of digital abuse.

Specifically, our research seeks to understand two areas of this digital-safety landscape:

RQ 1: What is the broad context of digital-safety threats youth experience? For example, what attacks do they experience? What potential harms do they face? Who are the attackers? What environments do the attacks occur in or across? How do experiences migrate across platforms and into the physical world?

RQ2: What protective practices do youth and adults who support youth adopt? What drives their decisions to adopt the practices? What factors affect when the practices are limited, evaded, or fail?

Participants described a complex digital-safety landscape that includes many more digitally-mediated threats, a wider spectrum of attackers, and more mi-

gration across platforms than has commonly been reported in the press or prior research (RQ1). Beyond social media, participants described threats mediated via gaming, dating, and financial applications ("apps") as well as by apps intended for users to engage with strangers (e.g., apps to "meet new friends"). These threats extend beyond cyberbullying and sexual violence, with participants describing dangerous threats such as pressure to commit illegal activities, financial fraud, and to spread misinformation targeted at youth.

Further, although a common picture is that certain threats are associated with certain attackers (e.g., sexual violence by adult strangers; cyberbullying by peers) [177, 63], participants described attacks being carried out by a variety of attackers. Sexual violence, for instance, could be perpetrated by adult strangers, family friends, other known adults, or other youth. Threats participants experienced regularly involved the use of multiple platforms; as threats progressed, the interactions between the youth and their attacker tended to move from popular platforms to more private, less-popular platforms. Threats could quickly escalate, spreading across social contexts and amplifying the harms involved. Youth susceptibility to attacks was influenced by psychological and social factors including marginalization and family instability. This wide and nuanced picture of both attackers and threats is one of the two main contributions of this work beyond prior research.

To prevent, mitigate, and respond to these threats, youth and adult participants described a variety of protective practices (RQ2) which may be familiar to parents and researchers: monitoring or restricting access to content, apps, and devices; assessing risk and imposing limitations on who youth communicate with; sharing information and resources when available; and (less commonly)

reporting incidents.

The second main contribution of this work centers around highlighting three key problems that reduce the effectiveness of these practices. First, youth and adult participants reported gaps in their knowledge of both threats and possible mitigations, along with a lack of resources for gaining that knowledge. Second, despite youth tending to be savvier about technologies than adults, youth are often not involved in the development and deployment of these practices, and may see adults' protective efforts as intrusive and autonomy-limiting, leading to a lack of buy-in and evasive behaviors that leverage their savvy. Third, the adults who support youth often don't work well with each other or with youth: they are not always up-to-date on the apps youth use, can be skeptical of others within the digital-safety landscape, and have limited communication with the other youth and adults who are involved (notably, around incident reporting). This leads to a lack of coordination and trust.

Together, our findings contribute to a relational understanding of the digital-safety landscape faced by youth around digitally-mediated attacks, adding nuance, complexity, and comprehensiveness to prior work that are important to consider in research, design, and policy efforts to support the digital safety of youth.

2.2 Related Work

We begin this section with a summary of prior work about the digital habits of youth. We then describe the known pathways to threats and harms to which youth are exposed and discuss common threats where technology plays a role.

We follow with a recap of efforts to protect youth from digitally-mediated threats, and conclude by describing how our work adds to this literature.

Evolving digital habits of youth. Youth today grow up with friendships and connections that concurrently evolve in the physical and digital worlds. More than half of teens aged 13–17 report having met friends online (57%) [129], over one-third (35%) have a close friend who lives far away, and 15% have a close friend they met online [15]. Furthermore, almost half of teens in the U.S. (46%) report being online "almost constantly," using many apps—*Instagram*, *Reddit*, *TikTok*, *Twitch*, *WhatsApp*, *YouTube*, and more—to consume content and connect with others [237]. Youth also use gaming and financial apps to communicate with others and pursue their interests and independence, and dating apps [142] to initiate romantic relationships. Technology facilitates rich social lives, exploration of identities and interests, artistic expression, entertainment, staying informed, connecting with social groups, and participating in online communities [39].

Pathways to digitally-mediated threats and harms. In pursuing these goals, youth are exposed to a number of threat pathways which have been classified into four categories of online risks [138]: (1) exposure to harmful online content (e.g., pornography), (2) unhealthy and dangerous contact (e.g., sextortion), (3) inappropriate conduct (e.g., harassment, cyberbullying), and (4) unsafe contract (e.g., financial fraud) [211, 138]. These threat pathways can lead to a broad range of harms that vary in severity from feeling upset or anxious to depression, self-harm, and suicide [14]. While digitally-mediated threats can affect anyone, youth are at a disproportionate risk due to their established tendency toward risk-seeking behavior [31, 7, 109, 212, 243] and limited understanding of the consequences of potential threats [241].

Pathways to threats can proliferate due to existing physical world vulnerabilities [138, 173], including unstable living situations, introversion, mental health issues, witnessing or experiencing trauma, disabilities, and immigrant or refugee status [207, 181, 131]. Many of these situations affect physical-world relationships and/or resources available to youth, which can lead them to seek new relationships online, potentially exposing them to more threats [173]. Youth with stigmatized or marginalized aspects of their identity can also face greater threats online. For example, prior work has explored threats experienced by LGBTQ youth [96, 59] as well as how safe spaces can become places where harmful interactions occur for transgender and gender non-conforming people [203].

Common digitally-mediated threats. Some of these threats have been explored individually. For instance, *teen dating violence* is a widespread public health problem in the U.S. [168], with around 1 in 6 high school students reporting having experienced physical or sexual dating violence [30, 76]. A growing body of work has examined how perpetrators of teen dating violence leverage technology, including monitoring a partner's activities, requiring that passwords be shared, or extorting youth into sharing sexual images [24, 65, 97, 141, 197, 230, 217, 215, 214, 216, 220, 246, 245, 224].

Another common digitally-mediated threat is *cyberbullying*: intentionally aggressive behavior that is repeatedly carried out in a digital context against a person who cannot easily defend themselves [176, 119]. Fifty-nine percent of U.S. teens report having experienced digital harassment or cyberbullying [14], often bias-based cyberbullying targeting individuals based on their social identity, which includes hate speech or gender-based violence [103, 100].

Efforts to protect youth. Complicating our understanding of threats is that

youth *need* to experience some risks to develop risk-coping mechanisms, particularly during early to middle adolescence (i.e., ages 10-17) [109]. According to Jia et al.'s risk-centric framework [109], youth learn risk-coping behaviors through digital risk-taking, thereby exposing themselves to risky situations and possible risk escalation. Youth risk-taking is also driven, in part, by seeking heightened stimulation and novelty combined with an immature self-regulatory system [212].

Parents often play an important role in managing risks for youth in the physical and digital worlds. Prior work has examined common approaches parents use to try to mitigate digital-safety risks for youth, including active mediation (e.g., discussing online safety), restrictive mediation (e.g., setting rules), and technical mediation (e.g., monitoring and parental controls) [132, 136, 104]. A smaller body of work has focused on youth, engaging them around designs to help youth manage threats like cyberbullying [19] and non-consensual sharing [200], and respond to harms suffered [248].

How our work adds to the literature. While much is known about specific types of digitally-mediated threats directed at youth, and some work has explored how to help protect youth from the perspective of parents as well as youth themselves, the HCI community lacks a comprehensive picture of the threats, attacks, and protective practices youth experience online today—gaps identified in a recent review of youth risks and harms online [213].

The identification of these gaps has emphasized the importance of delineating the broader context of digital-safety threats youth experience by outlining the types of digitally-mediated threats and harms youth encounter, the types of attackers and complex relationships within which attacks occur, the digital

contexts in which the attacks occur, the role of technology in facilitating or preventing threats, and the psychological and social factors that affect youth susceptibility to digitally-mediated threats (RQ1).

Similarly, it is important to map the protective practices that youth and the adults who support them engage in—reaching beyond parents to include other adult stakeholders such as educators and advocates—studying the challenges faced by each and the interactions between them, as well as better understanding the role of youth themselves in this wider protective ecosystem (RQ2).

To do that, we will draw on the perspectives of different stakeholders to reconstruct a landscape of digital threats, risk factors, and preventive factors in the stakeholders' digital youth safety ecosystem. To this end, we pose the following research questions:

2.3 Methodology

To build this broader perspective, we conducted a qualitative study that involved semi-structured interviews and focus groups with 36 youth and 65 adults from 13 states[2] across the U.S. This large number of participants was needed to include youth with different backgrounds who had varying experiences with digitally-mediated attacks and harms, and to better-understand the perspectives of the many adults who support youth[3]. We collected data from October 2021–May 2022, during which several COVID-related restrictions were in place. Interviews and focus groups were conducted remotely via phone or video conference.

[2]States included AZ, CA, CT, IN, FL, MA, MI, MN, NY, OH, OR, TX, WI.

[3]This includes parents, teachers, health professionals (physical and mental), and advocates for youth targets of attacks.

2.3.1 Youth participants (N=36)

Recruiting. Our 36 youth participants were aged 10–17. We recruited them from three groups, chosen to broaden the kinds of experiences with digitally-mediated threats and harms we might learn about from participants. Youth from *Group 1* (n=15) received crisis intervention, counseling, or other support from social service agencies. All youth in Group 1 had experienced or witnessed domestic violence, sexual violence, and/or child abuse. Youth from *Group 2* (n=11) participated in school-organized programs about healthy relationships that aim to help students identify destructive patterns of behavior[4]. Youth from *Group 3* (n=10) had experienced or were experiencing digitally-mediated attacks or harm; they self-selected to participate in our study. To the best of our knowledge, youth in Group 3 did not receive support from social service agencies or participate in school-organized relationship programs.

Participants from Group 1 were recruited with the help of the social service agencies. To recruit participants from Groups 2 and 3, we met with leaders from public and private schools, after school programs, school-organized healthy relationship programs, and community groups. Recruitment flyers were distributed by organizations, schools, parent groups, and a website that provides digital citizenship education for middle-school-aged children. Youth also learned about the study through word-of-mouth. The youth participants attended public (n=33) or private (n=3) school and were from diverse socioeconomic backgrounds. Twenty-four identified as female, 8 as male, and 4 as non-binary. All youth participants received a $25 USD e-gift card as a thank you.

[4]Generally, the mental health professionals who lead these programs are not *mandated reporters* who must report abuse to authorities, perhaps creating a more open environment for youth to share information. Also of note is that most of the programs did not specifically cover digitally-mediated threats.

Data collection. We conducted 10 semi-structured interviews and 8 focus groups. Interviews lasted 30-90 minutes, while each focus group—comprised of 3-6 participants—lasted 30-60 minutes[5]. Many participants noted that their first discussion about digitally-mediated threats occurred during their study session.

Each session started with the lead researcher reviewing the consent form, reminding participants that they did not have to answer our questions, the session was being recorded, they could request we stop recording at any time, and that they could leave at any time without providing a reason. In all cases, they would still receive their thank you gift. Two participants chose not to be recorded; detailed notes were taken in their sessions.

2.3.2 Adult participants (N=65)

Recruiting. We recruited 65 adult participants who help youth prevent, mitigate, or recover from digitally-mediated attacks. Nineteen were *parents* of youth (15 identified as female, 4 as male). Forty-six were *professionals*, that is teachers, librarians, school nurses, mental health professionals, advocates, physicians, or lawyers (33 identified as female, 7 as male, and 6 as non-binary)[6].

To ensure that we included a diversity of perspectives, we used multiple recruitment approaches. We promoted the study at events and to relevant groups, emailed people who expressed interest, distributed paper flyers, and advertised the study on the aforementioned website. We also used snowball

[5]Two focus groups met twice at the request of the youth.

[6]In some cases, participants had intersecting identities (e.g., professionals who were also parents of youth or were themselves youth survivors). When this surfaced, participants were asked how they wished to be represented.

sampling, utilizing referrals from previous participants. Each adult participant received a $25 USD e-gift card as a thank you.

Data collection. We conducted semi-structured interviews with 57 participants[7] and three focus groups totaling 8 participants. Each interview and focus group lasted an average of 60 minutes. Participants in the focus groups requested the group format. One was comprised of members of a parent group; the other two were comprised of professionals from the same organization. At the beginning of each session, all adult participants received the same aforementioned reminders that youth participants received. All sessions were recorded with permission, except for three interview sessions in which participants chose to not be recorded; detailed notes were taken in those sessions.

2.3.3 Discussion guides

Discussion guides for youth and adult participants were structured around our RQs of understanding the breadth of threats and protective practices, the context around them, and the factors that impact them. The same discussion guides were used for focus groups and interviews, although they varied slightly depending on whether the participants were professionals, parents, or youth.

For the professionals, we asked about the kinds of digitally-mediated attacks and attacks they most often dealt with, along with examples of both attacks and technologies involved in them. We also asked about their knowledge of those threats and technologies, as well as protective practices around them. Finally, we

[7]Two *parents* and 3 *professionals* participated in two interviews each at their request, for a total of 62 interviews with 57 participants.

asked about the advice and resources they give to others and have available for themselves, including their perceptions of others involved in youth digital safety. For parents and youth, we asked similar questions, but with a focus on their own experiences: the attacks and harms youth had experienced, the platforms and apps they used, and their assessment of each other's knowledge of threats and technologies. Our discussion guides are available in supplementary materials.

2.3.4 Data analysis

To analyze our data, we used an inductive thematic analysis [41] approach. We began with a comprehensive reading of the transcripts and written notes. Following this reading, three coders performed an initial pass of the data by open-coding across each transcript line-by-line. We determined that youth and adult participants should be analyzed separately so that identified themes could be compared.

Codes for youth and adult participants were maintained in a shared codebook. The three coders met frequently to resolve discrepancies and condense the codes. Three additional passes were conducted over the data until coders were satisfied the corpus had been covered. We then clustered related codes to identify commonalities; this resulted in the themes that form the backbone of Section 3.4.3 and Section 2.5.

2.3.5 Safety, privacy, and ethics

Given the sensitive nature of our study, we took many steps to help ensure safety, privacy, and ethics.

Study preparation and review. Before engaging with youth participants from *Group 1*, we met with experts from each organization that participated in our study. We iterated with them to refine our scripts and procedures for engaging with youth (e.g., timing, protecting identities). These scripts and procedures were also used with *Groups 2 and 3*. The entire study was approved by the lead author's IRB. In total, preparation and review took place over several months and involved input from many experts.

Informed consent. For youth participants from *Group 1*, informed consent was obtained prior to their session by staff at the respective social services agencies. Youth participants from *Groups 2 and 3* were provided with a consent form via their school, organization, or parent. Parental consent did not require the youth's name to be listed on the consent form to protect the identity of the youth in cases in which the youth did not want their name recorded. In the one case in which the youth's name was not included, parental verification was confirmed by the school or organization the youth attended. Forms were obtained from schools or organizations or directly sent through a dedicated secure research email. Oral consent was obtained from the youths at the start of their session. All adults provided oral consent and were provided with a consent form.

Safety and anonymity during sessions. The first author, who has received trauma-informed training, conducted all interview and focus group sessions. Each participant from *Groups 2 & 3* had the option to include a licensed mental

health or other professional from their school/program, or a parent. All participants from *Group 1* participated via focus groups as recommended by the social service agencies. Each group was comprised of participants who knew each other plus 1–2 licensed mental health professionals they knew.

The names and likenesses of all participants from *Group 1* were unknown to the research team (the video conferencing software displayed pseudonyms, cameras were off)[8]. With the consent of the Group 1 participants, the mental health professionals provided their age and context to the first author. Youth were asked to confirm that they were between the ages of 10–17 per the study protocol. All youth chose to share their age.

All *adult participants* had the option to participate anonymously; none chose that option.

Data clean-up and sharing. To further protect participants, we do not mention the names of partner organizations, schools, or agencies. We removed identifying information about the participants or the people they mentioned from all session recordings, notes, and transcripts. When reporting our findings, we omit unique details, phrases, or words from quotes to mitigate identification.

2.3.6 Limitations

We acknowledge that our study has several limitations. Though large for a qualitative study and involving multiple perspectives, our 101 participants do not

[8]To help preserve anonymity, recruiting and consent for *Group 1* participants was facilitated by the licensed mental health professionals; the lead author only had direct contact with Group 1 participants during the sessions.

represent all experiences, family situations, stakeholders, or support structures that might affect the digital-safety experiences of youth. For instance, although law enforcement and non-parental caregivers are part of the digital-safety landscape, they were not part of this study. Further, our focus was on the experiences of targets and those who support them; we did not explicitly recruit attackers. We note that among our youth participants, we found that the same individual youth could be the target of an attack in one situation and an attacker in another. A deeper study of attackers would add to the literature if it could be done in the face of recruiting and ethical challenges involved.

We also did not compare experiences between the different groups of youth we recruited. We did not set out to do a comparison study, sampling instead for breadth of experiences. Participants also primarily identified as female, which may lead to gaps in our findings since digital abuse affects youth of all genders. Further, threats and harms may also vary based on gender. Future work aimed at teasing out potential differences between groups and genders would make useful contributions beyond what we report here.

Finally, all of our participants were U.S. residents. Although we have some geographic diversity with youth participants from 5 states and adult participants from 13 states, experiences may differ across countries, cultures, locations, types of schools, and other aspects of context. This study is also subject to standard limitations of self-reported data, including recall and observer bias.

	Adults (N=65)	Youth (N=36)
Harassment toxic content, content leakage, impersonation	41	31
Sexual violence non-consensual intimate imagery, requests for explicit content, sexual abuse & grooming, sex trafficking	47	26
Coercive control & stalking surveillance, account access	20	17
Unsafe & illegal behaviors viral challenges, purchase of illegal goods	17	13
Financial fraud online scams, extortion schemes	4	8
Misinformation & deepfakes fake news, deepfake techniques	5	4

Table 1: Number of participants who mentioned at least one attack in each category discussed.

2.4 Threats Experienced by Youth

The diverse digital habits and contextual risk factors of our participants led to a complex digital-safety landscape. We identified several categories of digitally-mediated threats experienced by youth, including harassment, sexual violence, coercion, unsafe and illegal behaviors, financial fraud, and misinformation (see Table 1).

In this section, we explore the nuanced relationships between these threats, the platforms and relational contexts within which attacks occurred, and the resulting harms to youth. We find that attacks are often interconnected—escalating and migrating across platforms and sometimes between digital and physical worlds. Further, in many cases, youth experienced more than one threat concurrently.

A note for readers. Some quotes, accounts, and findings refer to physical or sexual violence among youth, and may be disturbing.

2.4.1 Harassment

Many youth and adult participants described situations in which youth were harassed by peers, intimate partners, acquaintances, and strangers. Tactics included cyberbullying via toxic comments, impersonation, and content leakage. Harassment often resulted in emotional and relational harm to the targeted youth, but could also result in physical harm.

Toxic content. Youth described attacks on social media, gaming, and messaging platforms in the form of text, image, and video communications. These attacks involved name-calling, unwanted sexual requests or content, threats of digital harm (e.g., claiming to know the target's IP address where an attack could be carried out), or threats of physical harm (e.g., on school grounds). These attacks raised concerns about emotional and physical safety, often leaving youth feeling as if they had no way to protect themselves.

> "*When I'm at school and go on social media, I can see kids talk about me. If you don't dress a certain way, you're called a "bum" or a "dirty dusty." People think that if you don't have certain things that other people do—that you're less than them.*" – Youth, P71

Impersonation & content leakage. Youth also reported impersonation, often by peers, where attackers created fake accounts or profiles to bully the target and

disseminate abusive content to the target's social networks. This could escalate quickly across social circles and schools. One parent described a scenario in which her daughter was humiliated and bullied by peers; those peers created an account impersonating her daughter, so that it appeared as if images were being shared *by* her daughter.

> "*Two girls set [my daughter] up... While she was sleeping, the girls wrote all over her and put shaving cream in her hair. They used red marker to write horrible names on her, then photographed her. Then the girls created a Snap account [impersonating my daughter] and sent the pictures everywhere. I called their mom. I saw the pictures and felt sick. The mom said it was just a joke.*" – Parent, P62

Youth also reported doxxing as a way peers might attack.

> "*Some Discord school group chats are pretty calm, and then some of them are super, super mean. If you do something to a person that they don't like, they will doxx your [home address] and then your IP address.*" – Youth, Y82

Escalation of harassment. Youth participants also described how harassment escalated and crossed contexts. Conflicts starting in school would sometimes transition to social media and expand to broader friend groups. Social media was used to organize fights and amplify humiliation to a wider audience. Stories or videos from physical-world interactions often transitioned to the digital world, evolving into an escalating cycle of cyberbullying. This interplay of digital and physical violence came up many times during conversations with our youth *and* adult participants.

> "*If I had a little disagreement in class or something, then I go on Facebook and I'm like, "Wow, [name] should have never been saying that shit to me." It's like, alright, I'm calling her out now. I'll fight her, then it'll be put on Snap so everyone knows.*" – Youth, Y96

These escalations often involved single-purpose "clapback" accounts used to say disparaging or otherwise harmful comments about someone in retaliation for a perceived attack. These accounts were often a response to an attacker saying something offensive about the target in the digital or physical world. These clapbacks sometimes led roles to shift quickly, with attackers becoming targets and targets becoming attackers. Parents sometimes got involved.

> "*The school called us in... They said my daughter created a fake [clapback] Instagram account... It got to the point where that family told their daughter to hit my daughter in the face on school grounds. And they kept targeting my daughter. It was like a wolfpack mentality.*" – Parent, P30

2.4.2 Sexual violence

Another large class of threats centered around sexual violence. Participants described experiences with non-consensual intimate imagery, requests for explicit content, sexual abuse and grooming, and sex trafficking. Attackers were parents, other family members, peers, or strangers, spanning digital and physical worlds. Sexual violence often resulted in emotional as well as relational harm to the targeted youth, but could also result in physical harm.

Non-consensual intimate imagery. Youth described how sharing intimate images with relationship partners was often normative within their social circles. However, youth often did not anticipate that a relationship would end and that such images might be leaked. When that happened, youth experienced regret along with relational and emotional harm. Some intimate images were recorded by a relationship partner *without* the target's consent, then later shared after the relationship ended.

> "*Kids send nudes to each other, and sometimes girls end up getting exposed. I don't feel like a lot of people actually stand up and go to the police about it. Most times, it's the person that they're dating and you know, if the person is childish enough after y'all break up ... they'll just show people and send it around just cuz that's what kids do.*" – Youth, Y81

This could lead to non-consensual viral dissemination of intimate imagery with little recourse for the target.

> "*Once your nudes get sent out, you're done. It's going to spread. There's no way you can stop it. I've seen videos spread from state to state in literally 5 minutes. It's crazy. So, once they're out there, they're out there.*" – Youth, Y77

Requests for explicit content. Advocates explained how attackers pay youth for content—sometimes explicit content—through digital platforms. To reduce suspicion, attackers often initially connect with youth in ways that align with youth's understanding of normal platform use. For example, an attacker might comment on or like a youth's video, or request to exchange gifts for content that

seems innocuous (e.g., an attacker might ask a youth to create and send a video of the youth dancing or a selfie of the youth dressed in a certain way). These seemingly innocuous requests often escalated to more manipulative or explicit content over time.

> "*People gift for great content on TikTok. Someone may comment on your dancing. The person wants to help you. They tell you to share your [bank] account. The person then gives you gifts. We call them 'gifters'—people who gift. Some ask for my Instagram accounts, or pictures, or videos.*" – Youth, Y66

Some youth—particularly those from disadvantaged households—sold nude images for financial support.

> "*I've known quite a few people who meet random people on a Snapchat. The random people would offer them money for nudes. They would try it, and it would work. I know kids who try to sell their nudes too.*" – Youth, Y75

Sexual abuse and grooming. Advocates described sexual abuse perpetrated by known adults such as family friends or extended family members who knew the youth, sometimes residing in the same home as the youth. The attackers would engage in a duplicitous relationship with the youth, connecting with them on social media or using a second phone to communicate with them without other family members knowing.

> "*In child sexual abuse, [the attacker] is typically a family member or someone who is close to the family. Sometimes they call that person "family," but*

they're not actually blood. They're typically people who [the youth] trusts and are in some type of financial crisis. That community wants to show up for one another and house one another. Unfortunately, it also provides access for really vulnerable young children to become sexually abused. Social media makes this easy to do and easy to hide." – Advocate, P3

Outside of family, advocates and youth discussed how attackers—predominantly unknown adults—would create fake accounts where they posed as a youth, learned about and befriended the target, and then began a grooming process of the target via messaging applications or social media. This grooming period could last for several months before the attacker would request to meet the target at a public place, so as to not raise suspicion.

"*That's how they start reaching out to youth—in private messaging saying, "Hey, do you know so and so?" And then the youth can be like, "Oh yeah, from school." And the attacker will say "I'm friends with them too." Depending on how smart the attacker is, they'll really do their research on what this particular youth likes... Then eventually, they say "Let's meet up somewhere.*"" – Advocate, P50

Participants also described situations on gaming and dating platforms where attackers sought to connect, in some cases with full knowledge that the target was a minor (i.e., under age).

"*It's pretty common for youth to go on dating apps. If you're an attacker who has a sexual interest in youth, then it's an easy target because it's technically not illegal for you to go on it and seek out youth... The attacker will say, "If they're on Tinder, I'm assuming they're 18 or older.*"" – Advocate, P13

Sex trafficking. Advocates discussed sex trafficking—in which attackers forced youth to engage in sex with strangers—often involving youth from disadvantaged families or who experienced housing instability.

> "*Attackers know to offer underprivileged kids—who are under very stressful economic home situations—incentives or a way to get them out of the poverty or the struggles they're dealing with. Sometimes kids realize that their parents are struggling financially. Their attacker may offer to pay rent for their parents, may offer to pay for cell phones that their parents can't afford. So obviously for them it's like, "Okay, this is me taking a burden off of my parents' plate.*"" – Advocate, P2

Youth who were being trafficked were directed by their attacker to recruit other youth in person and online.

> "*Basically, another youth groomed me, and I thought it was normal. I was around older men because she was around older men. Our [adult attacker] basically manipulated her to tell me what to do. So, I could be on the market [i.e., trafficked].*" – Survivor/Advocate, P53

2.4.3 Coercive control & stalking

Advocates, legal professionals, and parents described forms of coercive control or stalking experienced by youth, often in the context of relationship violence.

This usually took the form of account access or digitally-mediated surveillance.

Account access. Many youth expressed that they felt they had to provide device access or their partner would accuse them of cheating or threaten to end the relationship. Similar to intimate partner violence, one of the defining aspects of youth relationship violence is emotional or psychological abuse, including controlling and jealous behaviors.

> "*Technology is used for monitoring in relationships. Students come up to me and say that they had to give their partner access to their social media, and that they have to let their partner check their text messages, phone calls, who they are talking to. Basically monitoring them like they're a parent to make sure they're not talking or flirting with anyone they're not supposed to.*" – Mental Health Professional, P24

Surveillance. In some cases, youth were used as a proxy in situations of intimate partner violence where one parent (attacker) would use the youth's device to monitor and track the youth's other parent (i.e., the attacker's ex-partner). For example, attackers used the youth's device to find the location of a shelter, or manipulate the youth into revealing information about their other parent (i.e., the ultimate target of the attacker).

2.4.4 Unsafe & illegal behaviors

Youth described situations where pressures to fit in led them to engage in unsafe—and sometimes illegal—behaviors. Tactics included encouraging youth to participate in viral challenges or purchase illegal goods (e.g., drugs or weapons).

Viral challenges. Parents and educators explained that some viral challenges were quickly adopted by youth. Such challenges often involve someone recording themselves while performing a particular task, then posting their recording, tagging it with the challenge name.

Challenges sometimes promoted illegal behaviors such as vandalism. For example, one teacher told us about the "Deviant licks" challenge that encouraged the destruction of school property:

> "*There was a 3-foot water pipe on the ceiling. [A youth] pulled it, and it flooded the bathroom. That [youth] got expelled.*" – Teacher, P4

Viral challenges could also be dangerous, and in extreme cases, fatal. Two parents shared that they each tragically lost their child to a "choking challenge" which encouraged youth to achieve a brief high via self-strangulation. Youth approached these challenges as games, without awareness of the potential for severe harm.

These parents had used parental control apps and often talked with their children about social media; however, the parents didn't know about viral challenges.

Drugs & weapons. Participants also shared incidents where youth were encouraged to procure drugs, other illegal substances, or weapons online. The purchase of drugs was often motivated around parties and fitting in.

> "*At a sleepover, the youth attendees purchased edibles [containing Tetrahydrocannabinol (THC)] from a stranger online. They said they were going out for ice cream; instead, they picked up the edibles.*" – Physician, P32

The purchase of weapons was often motivated by concerns for physical safety at school.

> "*When the kids get caught with a knife, they say they're afraid—it's for defending themselves. That's their excuse... The kids buy stun guns on Amazon. If it's illegal in their state, they have it shipped to a friend in a nearby state or have a relative from another state order it for them.*" – Teacher, P16

2.4.5 Financial fraud

Youth with digital cash or payment apps experienced financial fraud via online scams and extortion schemes. Examples included being tricked by content creator impersonators sharing scam links, hijacked accounts of friends' that sent requests for money, or strangers who would reach out and share a "tragic situation" the youth could help with. Once they realized they had been "tricked," youth sought external help (e.g., a parent, law enforcement, platform support) to recover from the attack.

> "*The attacker told me she was a 27-year-old single mother. She told me she needed money for her child. I gave out my bank card and also my online banking code. She wanted me to send money to PayPal. When I stopped, she started harassing and threatening me.*" – Youth, Y68

Advocates shared that youth often help their less-tech-savvy parents manage finance, school, and health applications, often with access to accounts that led to mistakes and the temptation to engage in illegal activities.

> "*Immigrant youth are often "parentified" because they set up all the accounts... We had a 16-year-old that set-up four bank accounts [in their parent's name] to sell drugs. The kids control the technology. Youth can use this for the wrong reasons... parents don't realize that giving their child so much access to their personal information is just setting up a dangerous situation for them and their child.*" – Advocate, P3

2.4.6 Misinformation & deepfakes

Compared to the above attacks, teachers and youth only briefly mentioned encountering misinformation, often in the context of social media. Teachers discussed how this was particularly challenging given the media habits of youth.

> "*My students get their news from TikTok. How can they know if it's fake news?*" – Teacher, P36

Related threats employed tactics used in mis- and disinformation campaigns, including the creation of fake accounts and content in the pursuit of harassment and sexual abuse.

"Deepfake" technologies that synthesize or alter visual and audio content allowed deceptive attackers to pose as youth themselves.

> "*There are people [online] who are much older than you: adults. But they use voice changers that make them sound much younger. For someone like me, I just play. And I just meet someone random, and they just say that they like me. And it really gets me uncomfortable.*" – Youth, Y89

2.4.7 Summary of threats

Our findings regarding the digitally-mediated threats youth experience illustrate a wide range of attackers. They include youth and adult strangers the targeted youth met online, peers, friends, current and former intimate partners, family members, and extended family members. The attacker's relationship with and access to the targeted youth—such as physical proximity at school or home, being in a position of trust, or being able to connect in a relationship-building context like a dating app—influences the attacker's capabilities and range of possible threats they pose.

Overall, threats led to a broad spectrum of harms youth might experience. Concerns centered around safety in the digital and physical worlds. They included emotional distress, sexual and physical violence, drug abuse, and self-harm including—in the most extreme cases—death. Youth experienced embarrassment, regret, helplessness, trauma, depression, loss of friendships, and more from digitally-mediated attacks. Stigmatization also affected youth, with broader social groups engaging in victim blaming, rumors, social ostracism, and isolation. The fallout from attacks sometimes extended to parents or caregivers who were blamed for not providing better protections for youth.

2.5 Protective Practices

Parents, advocates, teachers, schools, and youth themselves implemented protective practices in response to the aforementioned threats. Many focused on mitigating threats by managing the use of technologies, as well as monitoring

and restricting access to risky content, apps, devices, and people. Other practices emphasized prevention of (e.g., information sharing and education) and reaction to (e.g., reporting mechanisms) attacks.

2.5.1 Managing content, app, and device access

Schools and parents employed many strategies to manage youth access to risky content and platforms. Some schools forbade use of or required students to surrender their devices during school. Many schools leverage network appliances or endpoint agents installed on school-issued devices to prohibit access to social media sites, sites with explicit content, and other sites deemed harmful. Schools shared reports with parents and advocates, demonstrating the interconnected nature of the stakeholder safety ecosystem.

> "*The school monitors the WiFi. To access the WiFi, you have to log in with a student number. They see what kids are looking at. Once they realize a youth is looking at porn, they notify parents.*" – Advocate, P1

At the same time, schools' protective practices exposed tensions with youth, who described the monitoring as invasive and ambiguous. No participant had a clear understanding of exactly what was monitored on school devices or if monitoring extended beyond school hours (e.g., when youth might want to use the device for personal purposes because, besides their phone, it was often the only computing device they had access to).

> "*The teachers say, "Don't post anything inappropriate, because the school can see. Your principal can see." They warn us.*" – Youth, P101

Like schools, parents used monitoring tools and restricted access to apps and devices. They also employed strategies such as non-intrusive inspection by friending or following youth in apps. Youth found this to be more palatable than other types of monitoring.

> "*My mom added me on Instagram and Facebook. She doesn't want to log into my account. I don't think many teenagers would actually allow that. It feels like they are invading my privacy.*" – Youth, Y79

Parents were aware that their restrictions could create tension for youth who were striving for autonomy.

> "*I find it hard to take high schoolers off social media, because their identity is created on their page. If you take the phone away from them, they become borderline psychotic.*" – Parent, P30

Youth used several tactics to circumvent access restrictions: deleting then later re-loading apps, using steganographic apps, hiding or altering app logos, using secret alternate accounts or devices, making backups to circumvent device resets, using friends' accounts to elude device and platform restrictions, manipulating their phone's clock to evade time-limiting software, and using VPNs to avoid network-based restrictions. They often learned about these tactics from peers or online videos. These behaviors highlight a knowledge gap between youth and the adults who are trying to implement protections for youth.

> "*At the end of the day, if the parent forces it, the child is just gonna find a way to be sneakier. It may be making a new account or even getting a "trap"*

phone ... When kids feel parents are doing that just to be in their business and be controlling ... super strict parents just raise sneakier children." – Youth, Y80

2.5.2 Managing interactions

Beyond restricting access, youth and parent participants engaged in protective practices aimed at mitigating threats from specific attackers. Once they realized the potential for danger, youth might mute or block contacts. They also attempted to assess the authenticity and intentions of people they interacted with; this was complicated by anonymous or pseudonymous accounts and technologies for modulating voice or manipulating imagery:

"*The problem with avatars is that you don't see faces. People fake being 15 when they're 50.*" – Youth, Y89

Some parents sought to vet people a youth would talk to, either through talking about them with youth, or observing their interactions. If enough interactions were concerning, parents might enact strategies described earlier.

"*[The game has] this sidebar for talking to people. It's almost a chat box. I was always lurking nearby, asking "Who's that? Who's that? Who's that?" I blocked the game from my daughter permanently because of what happened with people talking to her. She doesn't play that game anymore.*" – Parent, P12

However, as with other controls, youth could circumvent vetting and blocking. For example, they would give suspicious or forbidden contacts unrecognized names to avoid parental scrutiny, while platforms that parents had more control over were abandoned for platforms that parents were less aware of or concerned about.

2.5.3 Location monitoring

Because some threats transitioned from the digital to the physical world, youth and parents sometimes used location services to mitigate threats involving physical world attackers. Parents who used location tracking apps explained that their children traveled alone to school; they wanted to make sure their children were safe.

> "*I use Life360. I don't have to worry about some app using her camera and looking at her. I just want to know where she is.*" – Parent, P34

Youth frequently engaged in consensual tracking for safety purposes and for connecting with nearby friends, sharing their location with close friends via apps such as Life360, Snap Maps, and Find Friends.

> "*With some apps, you share location with close friends for safety, to see when people get to school. It's something you do. With Snap Maps, you can see everyone. Like, you might be somewhere and want to see if anyone you know is close by.*" – Youth, Y74

As with other protective practices, youth sometimes enacted workarounds (e.g., disabling tracking apps or using location spoofing software). They also might use multiple devices—some with tracking enabled and some without—to control who could access their location. Parents we spoke with were unaware of these circumventions.

2.5.4 Sharing information and resources

Youth and adult participants shared information about threats and protective practices with us.

Schools and advocates sometimes provided structured education to youth around abuse, internet literacy, and related concepts, attempting to reduce the chances of youth experiencing harm. However, these programs focused on general security hygiene—using strong passwords, performing vanity searches—rather than mitigating the digitally-mediated threats our study found.

> "*We don't have programming geared towards technological abuse. We focus on physical, in-person abuse. In terms of addressing it through counseling, we use what we know about physical abuse, then kind of remix it to better fit technology, because that's a whole different thing.*" – Advocate, P1

These gaps sometimes stemmed from school administrators' concerns around what's appropriate to cover in educational interventions.

> "*Ultimately, the Principal holds a lot of power. When we say, "Kids need these workshops" and they hear "sexual harassment," they say "We don't*

want that for students. They don't need to hear that." And I think to myself "Yes, they do."" – Mental Health Professional, P24

Outside of structured education, youth and parents learn about threats and advice via their own or their peers' personal experiences. For example, all youth participants had personally—or knew a friend who—shared an intimate image. No youth participants reported receiving education about sharing intimate images in school. Parents, similarly, don't seem to realize the extent of digitally-mediated threats that youth might experience.

"*We've seen children aged 7+ who have cell phones. Some parents have no idea what parental controls are... Parents think [the children are] only watching YouTube videos or talking to their friends on messaging apps.*" – Advocate, P3

2.5.5 Reporting attacks

Finally, youth and adult participants sometimes reacted to attacks by reporting them. Youth often turned to friends for support. It was less common for them to turn to adults due to concerns about how the adult might react. Regarding the effectiveness of more formal reporting—to platforms, schools, or law enforcement—youth and parents were skeptical.

"*When you report something, you're supposed to say why. I don't think platforms actually read [reports]. If they actually did—and looked at the account—more stuff would get taken down.*" – Youth, Y84

Parents and advocates shared that reporting to schools might lead to law enforcement or child protective services (CPS) getting involved, which can have negative consequences:

> "*If anything happens—let's say the kid is involved in an abusive relationship or sexual exploitation—the parents are worried they'll be blamed, and CPS will be called on them. So they don't report it. Our school system has a reliance on CPS that I disagree with, but it's the reality.*" – Teacher, P5

Even when parents or advocates *want* to formally report an attack, it's often unclear to them how to do it when the attack is digitally-mediated.

Instead of formal reporting, youth sometimes turned to social media. They might post screenshots of harassing messages, other details about the attack, and sometimes publicly disclose their attacker's name.

> "*People are increasingly turning to social media and public disclosures as a way of getting accountability, justice, and more of a feeling of control over their situation. They want to protect other youth, particularly young women. They want to share their story and get support.*" – Lawyer, P42

2.5.6 Summary of protective practices

These results demonstrate a wide variety of practices that youth and adults use to mitigate digitally-mediated threats: monitoring behavior and location; restricting access to content, platforms, and devices; providing or receiving education; and informally or formally reporting attacks. Effectiveness varied based on each

person's understanding of the threats and how to mitigate them. Protective practices focused on *prevention*—especially by parents—and *reaction*—especially by teachers, advocates, lawyers, and mental health professionals who often got involved after an attack had occurred. Youth themselves were aware of at least some digitally-mediated threats, and took action to mitigate them by implementing protections for privacy, safety, access, and personal boundaries, while seeking to preserve their autonomy.

Together, these practices—along with the youth and adults who support them—can be thought of as a *stakeholder safety ecosystem*. While they all have congruent aims for youth digital safety, their actions are often not coordinated, and are sometimes at odds with each other. For example, youth reported that they often didn't tell adults about their safety concerns, and they had received little to no education about digital safety. Furthermore, youth were often in conflict with parents or schools due to perceptions that the adults were trying to curtail their activities, invade their privacy, or otherwise introduce burdens that didn't seem reasonable to youth.

2.6 Discussion

Together, our findings provide a complex digital-safety landscape consisting of attackers, threats, and harms to youth, paired with the practices youth and adults employ to prevent or react to attacks. We structure our discussion along threats and practices. First, we present a comprehensive view of threats, emphasizing important relationships between attackers, targets, threats, and platforms, and the need to expand beyond single threats, platforms, or incidents. We then focus

on key issues that arise in trying to enact protective practices, highlighting how problems with knowledge, communication, and attention to the agency of youth can create conflict and reduce efficacy.

2.6.1 Dimensions of and relationships between threats

Our findings point to the need for research and design around the broad set of digitally-mediated threats—and their associated attackers—our participants reported. This includes more nuanced attention to the nature of the relationship between attackers and youth, moving beyond coarse attacker categories. It also includes distinguishing between multiple threats and considering relationships between them rather than in isolation. Finally, it requires addressing the complexity of threats that span platforms, time, and the digital and physical worlds while retaining the mechanisms that make technologies so important for youth.

Moving beyond coarse attacker categories. Even though prior work often highlights the relationship of the attacker to the targeted youth (e.g., cyberbullying by peers, distribution of non-consensual intimate imagery by a former intimate partner) [179, 70, 132], parents, schools, and digital literacy programs continue to simplify how they refer to attackers (e.g., as ”peers,” ”adults,” or ”strangers”). We found that the nuanced details of the relationship of the attacker to the targeted youth is quite important to understand—it can affect the threats youth face, the tactics attackers use, and the harms youth experience. Both peers and adults can be close friends or intimate partners of youth; both can be acquaintances or strangers of youth; and this matters. For instance, intimate partners and strangers might both pose threats around unwanted sharing of sexual content,

but the motivations and tactics are very different. We also found that adults with close proximity or relationships to youth sometimes pose much more dangerous threats to youth than adult strangers, exploiting proximity and trust in ways that make it difficult for others to notice abuse or for youth to report it.

Participants' stories suggested other important dimensions for reasoning about attackers, including groups of attackers versus individual attackers (groups being more common in harassment and cyberbullying, digital challenges, and sometimes trafficking) and local versus distal attackers (physical harms may be more common when attackers are close in proximity to the target). Further, the same individual can be a target in one relationship and an attacker in another, or face concurrent attacks within and across relationships. Our study identified these issues as important, but they were not our focus. Future work that investigates these dimensions of attackers and concurrency of roles and threats would be a natural and productive next step toward the comprehensive views of the digital-safety landscape that we and other researchers see as vital.

Distinguishing and considering multiple threats. Our findings also call for more precise terminology for threats and the need to consider multiple threats. This can support better communication; for instance, the common term "teen dating violence" does not adequately represent the variety of threats that can result from intimate peer-to-peer relationships and is not a term most youth seem to recognize. Careful terminology can also avoid conceptual muddling: for example, "sexting" lumps together consensual and non-consensual sharing of intimate images while collapsing multiple associated threats, including increasing the chances of non-consensual sharing or escalation to offline meetings that might result in physical harm.

Further, although sexual violence and cyberbullying rightly receive much attention, other threats don't, but need it. Youth were encouraged or coerced into illegal or otherwise unsafe behaviors around drugs, weapons, and recruiting for traffickers; experienced coercion and stalking similar to adults; and are likely to be increasingly affected by exposure to misinformation and other harmful content. This wider range of digitally-mediated threats needs to be addressed in protective practices, platform designs, and advocates' intake processes.

Threats cut across contexts. Participants also reported "attack journeys" in which attacks and harms occurred across multiple platforms, varying timescales, and even digital and physical worlds. Attacks often moved from more public to relatively private platforms. Youth sometimes did this intentionally, moving potentially risky interactions away from platforms where their friends, parents, or school might be watching. Attackers also intentionally leveraged multiple platforms—exploiting cases where youth link private accounts to public ones through their profiles or posts—to glean knowledge in public forums only to use it to find and befriend the youth in more private settings. These risks were often not apparent to youth or the adults who support them.

Threats also occur at multiple timescales. Though some attacks are instantaneous—like a stranger immediately requesting or sending unwanted nude pictures—others evolve. Cyberbullying can take days or weeks to create content and rally others to participate in the bullying; threats of sexual violence often take months as attackers slowly groom targets into relationships they later exploit. Over-focusing on the harm can reduce attention to the *process* of attacks. If better understood, these processes might be detectable or disruptable[9].

[9]We see some parallels to the security concept of cyber kill chains, where prevention and mitigation efforts aim at specific steps in an evolving attack.

Attacks appropriate legitimate features and goals. Unlike security vulnerabilities, which generally exploit unintended behaviors in systems, the threats we observed often appropriate features that have legitimate uses. For instance, linking private and public accounts across platforms helps youth manage audiences and identity disclosures, but can allow attackers to glean public information and infiltrate personal spaces. Pseudonymous accounts allow youth to conduct these activities at a distance from their main identity, while allowing attackers to do the same thing. Seeking information about mental health concerns and stigmatized interests can provide great value to youth, but disclosing personal information creates risk including bullying and harassment.

That said, there are cases where these features are very exploitable. In particular, some platforms advertise that they are age-appropriate for teens who want to meet other people, but appear to do little to verify identities or moderate activity, opening wide gaps for deceptive attackers to exploit. This can create unwarranted safety expectations because the contextual signaling (e.g., mental health forums, apps with a 12+ age rating) might suggest a protected environment that actually increases risk because the protection is illusory. Reducing illusions of safety is one concrete way to accomplish protective goals of making the digital-safety threat landscape clearer and more navigable for youth. More generally, incorporating design approaches that center adversaries and threats, such as security by design and privacy by design, could help platforms better-assess dangerous implications of otherwise-legitimate features and be more proactive in addressing them.

A relational view of threats to youth digital safety. Together our results call attention to the need for viewing potential threats to youth in terms of rela-

tionships: of relationships between attackers and youth, relationships between different threats, relationships between platforms that can exacerbate threats, and relationships between legitimate goals and unintended uses. Future work that synthesizes these results with other extant work from a relational perspective could have real value in advancing theoretical understanding of youth digital safety. We also see a relational perspective as a potential step toward advancing youth digital safety: identifying the most risky relationships between people, threats, and platforms could focus efforts on modifying or disrupting those relationships.

2.6.2 Key barriers to effective practices

Our second main set of findings calls out the range of protective practices and stakeholders—parents; advocates; educational, health, and legal professionals; along with youth themselves—that attempt to mitigate the threats described above. These practices include monitoring and restricting communications, content, platforms, and devices; assessing, discussing, reporting, and learning about risks; and seeking support from others. However, these practices are limited by gaps in stakeholders' knowledge of technologies and in resources available for gaining that knowledge, as well as by gaps in the alignment of interests, communication, and trust between stakeholders.

Knowledge gaps & lack of educational resources. Although youth were seen on balance as more knowledgeable than adults in the stakeholder safety ecosystem, all believed both themselves and others lacked critical knowledge about technologies and threats. Participants underestimated threats. For example, parents

perceived games as safe relative to social media despite in-game communication with strangers; youth were overconfident in their ability to detect deceptive attackers. Participants also expressed a lack of self-efficacy in using tools designed to mitigate threats, such as parental controls on content and screen time. Meanwhile, lesser-known platforms often escaped adults' radar entirely [237]; this made those platforms a source of additional threats, as well as a way for youth to evade protective practices they disagreed with.

These gaps are compounded by a lack of resources available for learning and teaching about digitally-mediated threats. Essentially every interview and focus group described needing more resources to help them understand what youth were doing online and how apps worked. The resources they had often did not adequately address actual harms and different stakeholders' needs. Schools often lack digital-safety educational programs, and those that exist focus on basics like account security hygiene or—contra the need expressed earlier for careful consideration of multiple harms—collapse a wide variety of harms into general concepts like "cyberbullying." Additionally, despite teen dating violence's prevalence and frequent occurrence on school grounds, 76% of high school principals surveyed say they do not have a procedure or policy in place to respond to incidents [115]. Platforms provide some information through help documents and related features, but most of these resources must actively be sought out.

Thus, there is a great need to provide accessible, actionable educational resources. Some resources exist, particularly for educators and youth. For instance, Common Sense Education's digital citizenship curriculum provides lesson plans with content and activities for both general digital safety and many of the specific

threats participants in our study described [107], while Social Media Test Drive provides youth with guided, simulated social media experiences that support experiential learning around digitally-mediated threats [61]. Other stakeholders are less well-served by existing materials, however. Advocates needed to know enough about digital harms to address them in their intake and counseling efforts, while medical professionals—including pediatricians and child psychiatrists—wanted to know best practices around mitigating digitally-mediated threats for both treating youth and advising youth and parents. The resources above were not designed to support those needs.

Coordination between stakeholders in the safety ecosystem. Another key barrier to protecting youth effectively is that stakeholders often did not work well together. Friction could arise from gaps in knowledge, for example, when parents' limited understanding of technology and advocates' limitations for considering technology during intake processes hindered their ability to work together. It could arise from gaps in communication, as described by youth who did not understand the monitoring and controls imposed by schools. It could arise from differing expectations about issues such as who is responsible for digital-safety education, with schools and parents often hoping for the other—or platforms—to take the lead.

Friction could also arise from conflict between stakeholders. Stakeholders sometimes had different perceptions of appropriate mitigations for threats, as illustrated by advocates who described the reluctance of schools to provide certain types of education around sexual violence. They also sometimes considered other stakeholders as unresponsive: youth, parents, and advocates alike were skeptical of platforms' responses to incident reporting. Some relationships were

also characterized by fear and hostility, as when parents and advocates described schools and law enforcement as aggressive, liable to blame families or victims, and overly willing to involve agencies that might disrupt their families.

Meaningful reporting and support. Participants were also quite negative about reporting incidents and concerns to other stakeholders in the safety ecosystem, describing skepticism, fear, and lack of capability. This makes improving the experience of reporting low hanging fruit for helping to improve relationships between stakeholders and mitigate harms for youth.

Advocates reported needing intake processes that made digital risks more salient for themselves and helped elicit more useful information about digital threats from reporters such as parents; our results provide a starting point for checklists of platforms, threats, and key attacker strategies that could enhance existing intake processes. Platforms might also stand to make reporting more valuable. When people report, they are often seeking (and hoping to give) help, justice, and support; reporting processes could emphasize this. For instance, platform reporting interfaces might connect youth with existing resources like crisis helplines that could provide immediate help in parallel with the platform's internal processes for handling reports. Making reporting processes simpler and more similar across different platforms and agencies—to the extent possible given different aims and constraints—might also increase people's ability to report and to coordinate when appropriate around reports.

Balancing youth protection and agency. Perhaps the most fundamental lack of coordination we observed is that youth tended to be treated as objects rather than participants in their own safety. Controls were often imposed by schools and parents, and especially in the case of schools, without consulting youth. There

appeared to be insufficient communication around these controls—how they worked, what was monitored, why it was done—which led youth to see them as intrusive or violating their privacy. This, in turn, led youth to use their relative savvy about technologies to evade controls using technical (e.g., VPNs), social (e.g., using friends' devices), and evasive (e.g., switching platforms) means.

Engaging youth as meaningful actors in their own digital safety would likely increase their buy-in to specific practices—hopefully reducing attempts at evasion—and their general awareness of the need to be agents in their own protection. It would likely support more appropriate balancing of protection and safety goals with youth's needs around communication, relationships, knowledge, support, and identity exploration. Their insights might also highlight aspects of app and platform design that are particularly risky, which in turn might guide efforts of platforms looking to create environments with less serious and more manageable threats. Since youth often know more about platforms and threats, the resulting practices might be more comprehensive and tuned to the actual risks youth face, risks they need to experience as part of developing their ability to manage threats in the future. Finally, a greater understanding of youth's perceptions and situational circumstances can help to inform policy and protections for youth digital safety [25, 102].

The need for communication and alignment. Our analysis calls out the need for better communication and alignment between stakeholders. Open communication lines are especially important in the face of larger social issues that can exacerbate tensions between stakeholders such as debates about sex education in schools, legal requirements to report harms, laws around regulating speech online, and differences in socioeconomic status that affect stakeholders' resources,

needs, and expectations.

Engaging with other stakeholders can reduce knowledge gaps, align expectations, and build trust. It can also leverage multiple sources of expertise to increase the chance of mutually beneficial and effective outcomes. We give specific examples around education, reporting, and increasing youth involvement and agency; our hope is that by emphasizing communication and building relationships between the many stakeholders involved in the safety ecosystem, other opportunities for better managing and mitigating youth digital safety will arise.

2.7 Conclusion

Through qualitative research with 101 youth and adults who support them, we've provided a complex digital-safety landscape consisting of attackers, threats, and harms to youth, paired with the practices youth and adults employ to prevent, mitigate, and recover from attacks. We have expanded on prior work by looking across the stakeholder safety ecosystem and describing moments of tension between youth, adults, and systems; showing how simple or popular narratives can occlude a broader range of threats with important contextual differences; and outlining how threats, attackers, and youth seamlessly move across platforms and into physical world harm.

We suggest that solutions focus on addressing this broad digital-safety landscape while improving coordination, communication and alignment, and access to up-to-date educational resources for youth and the adults who support them. We hope this work serves as a call-to-action for researchers and others who support the digital safety of youth to study and respond to a broader range of at-

tackers and threats through a relational lens, while also working to support youth awareness and agency in their own protection from the many digitally-mediated threats they face.

CHAPTER 3

AN INVESTIGATION OF TEENAGER EXPERIENCES IN SOCIAL VIRTUAL REALITY FROM TEENAGERS', PARENTS', AND BYSTANDERS' PERSPECTIVES

3.1 Introduction

Social virtual reality, also referred to as social VR, is a 3D virtual environment where users can interact with others through VR devices (e.g., VR headsets and controllers) [158, 80]. Social VR experiences are unique compared to those offered by other online spaces such as social media because of the fully immersive experience through voice, touching, and grabbing features using full-body or half-body tracking avatars [146]. Among all users, teenagers (between 13 and 17 years old) have become one of the largest user groups in social VR. Technology companies such as Meta are increasing their efforts to bring more teenagers to their social VR platforms as they represent the future of their user base [54].

Prior research has shown that teenagers face significant safety and privacy risks in social VR. For example, teenagers are exposed to violence, abuse, sexually explicit content, age-inappropriate content, voice trolling, and scaring, among others [185, 148, 148]. They are also exposed to traditional forms of bullying and name-calling, as well as unique forms of harassment that are specific to social VR, such as stalking individuals across rooms or worlds [150].

Despite the risks noted in prior literature, our understanding of teenagers' experiences with social VR and how to protect their safety, security, and privacy is still not comprehensive. We add to the literature by filling two significant

gaps. First, prior research has been focused on a single perspective in social VR (e.g., users, teenagers, etc.). However, as a complex social environment, a typical social VR scene often involves multiple stakeholders, such as teenagers themselves and other adult users. This multi-stakeholder perspective has not yet been addressed. These stakeholders co-exist and may interact with each other in social VR. They may have different, even conflicting perspectives on their social VR experiences. Such perspectives may also have an impact on how they behave themselves and respond to other risks and threats. Second, unlike adult users who can purchase VR devices by themselves, most teenagers receive VR devices as a gift from their parents. A clearer understanding of whether the parents are aware of the potential threats and risks their children may encounter when using VR devices is much needed.

In this research, we take a multi-stakeholder approach to study teenagers' experiences in social VR from the perspectives of three distinct stakeholder groups, i.e., teenagers, bystanders, and parents. *Teenagers* include youth who are between 13 and 17 years old. *Bystanders* encompasses users in social VR who are not teenagers. *Parents* refers to parents of teenagers who are social VR users. We aim to study the following three research questions:

RQ1: What threats are teenagers exposed to in social VR from the perspectives of teenagers, bystanders, and parents?

RQ2: What are the similar perspectives and tensions among teenagers, bystanders, and parents regarding social VR threats?

RQ3: What features do teenagers, bystanders, and parents desire to combat safety threats in social VR?

To answer these research questions, we conducted an interview study with 8 teenagers, 9 bystanders, and 7 parents. The interviews focused on participants' experiences in social VR, their perceptions and perspectives of the safety threats, and their mitigation strategies when facing these threats. Our analysis shows that some activities, such as Erotic Role Play (ERP, a type of role-playing activity that includes users decorating their avatars with components that have sexual orientation), are present among teenagers, yet many teenagers seem to have normalized such activities, and did not consider them as threats. On the other hand, most bystander participants evaluate the activities in social VR using the norms from our physical world and identified many types of risks that may jeopardize teenagers' mental and physical health. Parents generally showed a limited understanding of the threats that their teenagers may face in social VR, with many being aware of only a few potential risks. Our results highlight the discrepancies among the perspectives of three stakeholders, which may lead to conflicting social norms in social VR and possibly more significant risks for teenagers.

Our paper makes two contributions. First, we explored teenagers' experiences and safety threats from the perspective of teenagers, bystanders, and parents. This multi-stakeholder approach allows us to comprehensively examine our research questions with complementary opinions and experiences. To the best of our knowledge, this is the first study to conduct interviews with three distinct groups with a particular focus on their interactions with others and the identification of potential threats in social VR. Second, this study provides insights and design implications that aim to create safer and more fulfilling social VR spaces for teenagers. By drawing from the perspectives of parents, bystanders, and teenagers themselves, these implications can inform the design of future

social VR platforms and other online social spaces.

3.2 Related Work

3.2.1 Social VR: Benefits and Drawbacks

In social VR, users can create avatars that represent them in virtual spaces, then interact with others using their body gestures through full-body tracking (i.e., the body movement of a user's avatar corresponds to the body movement of the user in real-time) [34, 37, 210, 251]. This real-time embodiment allows users not only to customize their avatars but also pilot them with real-time gestures and motions [82]. In addition, social VR allows users to connect with each other and gather with friends from anywhere around the world and share experiences and activities that would never be possible in person [152, 159]. For example, they can watch movies in Bigscreen or play and/or create games in Rec Room. Another platform called AltspaceVR, which shut down in March 2023, offered varied activities such as interacting with people, attending events, etc. [10].

On the other hand, previous studies have highlighted that users of social VR platforms have experienced unpleasant experiences or have seen inappropriate behavior in virtual spaces. For instance, Blackwell et al. conducted an interview study with bystanders and reported that embodiment and presence in VR spaces make harassment feel more intense, and some features such as synchronous voice chat or avatar movements could trigger the risk of potential harassment in social VR [35]. Also, the results of Shriram and Schwartz's quantitative survey indicate that harassment was occasional in social VR platforms and that those in

female avatars reported experiencing it more [208]. Also, scholars have studied marginalized users and how verbal and non-verbal communication could lead to potential risks of online harassment [151].

Moreover, prior work has suggested that, among all users of social VR, children and teenagers are the most vulnerable [35]. This is due to the fact that interaction dynamics between adults and children in social VR introduce barriers, tensions, and frustrations due to the co-existence of mixed ages in this social space [150, 148]. Some adults have expressed concerns for younger users in social VR because of the prominent harassment risks [148]. Researchers have also observed incidents in which young people were exposed to inappropriate content such as sex, alcohol, and virtual sexual assault [147].

3.2.2 Technology-Facilitated Harassment

Among all issues teenagers may face in social VR, harassment is the one rising the quickest [186, 92, 58]. Abusive sexual behavior could have a profound impact on young people's mental and physical health (e.g., anxiety, distress) as well as on the development of their sexuality and social functioning, both in the short term and long term [44]. With the development of digital technologies, harassment and sexual abuse have also raised significant legal issues such as viewing or uploading indecent images of children or teenagers on the Internet or consuming of other child sexual abuse materials (e.g., text, images, child pornography, etc.) [92, 253, 86], cyber-bullying [247, 209, 73], and cyber-grooming [69, 144, 169]. Moreover, technologies may make it easier to initiate, escalate, and maintain abuse in various contexts [91, 164, 202], such as mobile devices [154], social

media [164, 187], gaming [91, 53], etc.

Numerous efforts have been made to combat online harassment in order to promote a safe environment for young users. For instance, some technology companies have designed and implemented various mechanisms to detect, prevent, and report sexual harassment [161, 16, 222, 85]. Research has also highlighted the opportunity to use automated computational approaches for risk detection to support children's online safety based on machine learning models [4, 6, 60, 167, 199, 11, 84]. Additionally, educational materials primarily targeted at parents have been developed to keep them informed about how their teens can stay safe when using social VR [160, 196]. Researchers have also been studying other ways to encourage teens to take action when experiencing harassment, like seeking peer support [95].

In this study, we build on prior work and focus on understanding teenagers' experiences and safety threats from the perspective of teenagers, bystanders, and parents. These complementary perspectives uncover nuances around teenagers' threats and point at opportunities for designing safety features and ensuring a safer and healthier virtual environment.

3.3 Methodology

To answer our research questions, we conducted a semi-structured interview study with teenagers, bystanders, and parents. We detail the study methodology in the following sections. This study is approved by our university's IRB.

3.3.1 Participant recruitment

We focused on recruiting three groups of users: teenagers (ages 13 - 17) who have experienced social VR, parents whose teenagers have used social VR, and bystanders (ages 18+) who actively engage on social VR platforms. In the context of this study, we use "bystanders" to denote individuals who are neither teenagers nor parents but may have witnessed other teenagers' interactions with others in social VR (similar to [62]). We do not consider bystanders in the physical world who may stand next to users who use VR devices. In total, we recruited 24 participants, including 8 teenagers (T), 7 parents (P), and 9 bystanders (B). Table 2 includes participant demographic information and their social VR experience. Overall, our participants represent diverse backgrounds in terms of their age, occupation, and location.

We posted our recruitment flyer on popular online forums (e.g., Reddit subforums such as r/VRchat, r/RecRoom, and r/Oculus), online communities (e.g., Discord), and interest groups on social media sites (e.g., Twitter and Facebook). Before posting it to these sites, we sent our flyer and IRB approval letter to the corresponding platform/group moderators for their review. We only posted the flyer after obtaining the moderator's approval.

Teenagers who were older than 13 years and were interested in our study were invited to fill in a screening survey through the link provided in our flyer. In the screening survey, we asked about their social VR experiences, the VR headset devices they have used, their frequency of using social VR, their ages, whether they have children, and if so, their children's ages.

Teenagers with stable access to a VR headset and social VR experience were

Group	ID	Gender	Age	Occupation	Location	Num. Kids	Usage Experience	Used Social VR Platforms
Teenager	T1	Female	17	Student	USA	0	2 years	VRChat, Rec Room Horizon Worlds
	T2	Male	14	Student	USA	0	2 years	VRChat, Rec Room
	T3	Male	17	Student	USA	0	1 year	VRChat, Rec Room
	T4	Male	14	Student	USA	0	2 years	Rec Room
	T5	Male	15	Student	Lithuania	0	2 years	Rec Room, EchoVR
	T6	Male	13	Student	USA	0	1 year	Rec Room
	T7	Male	13	Student	USA	0	1.5 years	VRChat
	T8	Female	17	Student	Belgium	0	2 years	VRChat, Rec Room
Bystanders	B9	Non-binary	47	Full-time employee	USA	0	1 year	AltspaceVR
	B10	Female	20	Caretaker	USA	0	2.5 years	VRChat, Rec Room
	B11	Male	21	Student	USA	0	1 year	VRChat, Rec Room
	B12	Female	22	Student	USA	0	1.5 years	VRChat, Rec Room HorizonWorlds, ChilloutVR
	B13	Male	23	Music instructor	Canada	0	5 years	VRChat
	B14	Female	21	Dance teacher	Canada	0	3 years	VRChat, Rec Room ChilloutVR
	B15	Male	20	Student	Japan	0	3 years	VRChat, Rec Room, Horizon Worlds, ChilloutVR
	B16	Female	NA	ASL teacher	USA	0	3 years	VRChat
	B17	Male	23	IT engineer	Brazil	0	1.5 years	VRChat, ChilloutVR
Parents	P18	Female	29	Lab manager	USA	1	1 year	AltspaceVR
	P19	Female	37	Housewife	USA	8	1 year	Rec Room
	P20	Male	41	Teacher	USA	1	1 year	VRChat, Rec Room
	P21	Male	35	Software engineer	Hungary	2	5 years	VRChat, Rec Room
	P22	Male	45	Architecture	Germany	2	2 years	VRChat
	P23	Male	53	IT project manager	UK	2	2 years	AltspaceVR, Bigscreen
	P24	Male	35	Pharmacist/ASL teacher	USA	1	3 years	VRChat, AltspaceVR

Table 2: Participants' demographics and social VR experience

eligible to participate as either teenagers or bystanders. Teenagers were those who were aged between 13 and 17. Bystanders were general users in social VR who are 18+ (we used "bystanders" rather than "users" as we were interested in their experiences as bystanders of teenagers' activities). Candidates who had both access to a VR headset and teenagers in their household who used social VR were assigned to the 'Parents' group. Although not required, all parents in our study had at least one year of social VR experience.

We did not limit our recruitment to certain geographic areas, as most social VR applications provide public places that can be accessed by users from any

region in the world. We required participants to be able to communicate in English.

3.3.2 Interview protocol

To accommodate the three participant groups, we framed the same interview protocol differently to account for the three different perspectives. Below, we describe the interview flow using the teenager version as an example.

The interview protocol consists of three parts. The first part focuses on the participants' background information (age, gender, etc.), their general VR experience, and their perceptions on social VR including their perceived benefits and concerns. The second part focuses on participants' behaviors and activities in social VR. We ask about their interactions with other users in social VR and how they approached/were approached by them. We then ask participants why they interact with other users and what their criteria are when they chose friends in social VR. In the next section, we focused on the risks and harms of social VR. We ask participants to share any negative experiences they encountered. Based on the participant's responses, we would either follow up with questions asking for more details or, if they did not have any negative experiences or could not think of any, we would ask whether they have encountered or witnessed any negative incidents, their opinions, and their reaction or strategies to navigate through those experiences. In the last section, we ask them whether they would like to see any features on existing social VR platforms.

3.3.3 Data collection and analysis

We conducted remote interviews via Zoom. The average interview length was 60 minutes and participants who completed the study received monetary compensation of USD $20 (or the equivalent value in their local currency). All interviews were audio-recorded upon participant consent and were then transcribed using Zoom's live transcription feature. We stopped the interviews when we did not observe new findings across all participant groups. As our study specifically focused on gathering teenagers' experiences from various perspectives, we reached saturation with a relatively small number of participants.

We then conducted a thematic analysis to identify repetitive patterns and themes in the interviews. Three researchers first selected one random transcription from our teenager participants as a sample. They closely read through the sample data several times to immerse themselves in the data, and then coded the sample independently at the sentence level using open coding. Upon completion, the three researchers discussed the coding results together and generated an initial codebook. They then repeated the same process on two additional samples, one from the bystander participants and the other from the parent participants. Through this process, the research team generated 3 separate codebooks, one for each participant group.

Following this initial coding, three researchers separately coded the remaining data using the agreed codebook. New codes that emerged from the data were added. In this process, the research team met frequently to discuss the coding results, and updated the codebook as needed. This process was done iteratively until all data was coded and full agreement was reached on the data from all three participant groups. All researchers then discussed and identified the themes for

each user group.

Since our coding process involved multiple iterations and discussions and reached a full agreement, intercoder reliability was not necessary [156]. Upon completing the thematic analysis, the research team further compared the themes across all three participant groups.

3.3.4 Ethical considerations

Since our study involved teenager participants, we took extra caution to ensure research ethics throughout the project, as described in detail below.

First, we asked all teenagers to obtain a parent's written consent before they could participate in our study. When we identified a qualified teenager from the screening survey, we sent them an assent form to sign together with a consent form for their parent to sign. To ensure that their parent was aware of their child's participation, teenagers were permitted to participate in the interview study only if they returned both signed assent and consent forms.

Second, before an interview with a teenager started, we always asked for separate oral consent from their parent. This is to verify that the teenager participants had indeed obtained their parent's permission to participate in our study.

Third, similar to the work done by Cranor et al. [56], when a teenager and their parents all reached out to us, we deliberately selected either the teenager or one of the parents to participate in our study (i.e., we only selected one participant from each household, thus the teenager participant and parent participant were

not in pairs). This intentional setup was to 1) respect the teenager's right to privacy, especially if they did not want to share their experiences/opinions with their parents; and 2) avoid potential embarrassment or conflicts among family members after participating in our study. 3) When the participants shared their experiences in social VR, especially those that were deemed to be sensitive (e.g., experiences related to harassment), we reassured them that their responses would be kept anonymous. We also instructed participants that they could skip any questions if they preferred and doing that did not influence their compensation.

3.3.5 Limitations

Our study has various limitations. For instance, we only interviewed 8 teenagers, 7 parents, and 9 bystanders who are English speakers. While we believe that our sample size is sufficient for our study, we recognize that there may be other types of safety incidents experienced by teenagers in social VR that are yet to be discovered. Additionally, we did not interview parents and children from the same family together to understand family dynamics. As mentioned above, we intentionally chose not to do so for ethical considerations.

3.4 Results

In this section, we present our findings on teenagers' social VR experiences. We focus on teenagers' experiences and potential safety threats from three perspectives, e.g., teenagers, bystanders, and parents. This section follows the four major themes we identified in our data analysis, including participants' general

perceptions of social VR, teenagers' relationship-building practices in social VR, teenagers' safety threats, and desired features. Given the qualitative nature of our study, when reporting the results, we used the terms "a few", "some", "several", "many", and "nearly all" to convey the relative sense of frequency rather than using specific numbers, similar to prior work [68, 89, 252].

3.4.1 Participants' general perceptions of social VR

Our participants from the three user groups demonstrated a consistent perception of social VR. Nearly all participants used social VR apps as a leisure activity to socialize, play games, and have intimate relationships in an immersive environment. Rec Room, VRChat, and AltspaceVR remain the most popular platforms among our participants. They were particularly drawn by several unique features of social VR platforms, such as real-time interaction, facilitating multi-modal communications (e.g., through voice, tone, body movement, facial expression, etc.), and the lifelike social environment. Additionally, many participants indicated that the full-body movement and the ability to support fluid non-verbal communication alongside verbal communication contribute to the unique experiences and made it more genuine to engage in various activities. These results echoed the findings from several prior work [151, 80, 150, 79], thus we only summarize them briefly. In the following sections, we focus on the nuances of this study and show teenagers' experiences from the perspectives of teenagers, bystanders, and parents.

3.4.2 Building and maintaining relationships in social VR

Compared to traditional 2D social networks, social VR provides a unique yet complex social environment, making it more challenging for teenagers to navigate through it. One common and fundamental activity relates to relationship building in social VR. Many teenager participants discussed how they have built and maintained relationships with other users in social VR, while many bystander and parent participants provided their observations to further uncover teenagers' practices.

In particular, while half of the teenager participants were able to bring their real-life friends into social VR for fun and interactive activities, the rest of them sought connections with new people. As a result, these teenagers were constantly involved in frequent and spontaneous interactions with strangers (i.e., people they have never met in real life). In this section, we present teenagers' strategies to develop and maintain relationships as well as their strategies to protect their own safety.

Various strategies to make friends

Being in a complex social environment in social VR, teenagers have developed their own strategies for building connections with strangers. When approached by other users, teenagers relied on several signals to decide whether to respond or not.

Appropriate avatar behaviors as a positive sign. With limited information available to judge other users' characteristics, their behaviors became the primary factor in determining whether one would be accepted as a friend in a virtual

world. The majority of the teenager participants reported that they preferred to make friends with those who exhibit decent and appropriate behavior. For example, T6 (13, male) mentioned that he may look for individuals who appeared to be respectful, kind, helpful, and avoid engaging in inappropriate or offensive behavior.

> "*I talked to them if they helped me with something, but if they're rude, I normally try to stay away from them, and most of the time in Gorilla tag, there's this button where you can mute people so that you don't have to listen to them.*" – T6 (13, male)

As T6's example highlights, interacting with others in social VR could be a complex and challenging experience. He developed strategies for interacting with others that prioritize his own comfort and safety. Furthermore, T6 took proactive measures to protect his own well-being such as muting rude people in social VR to create a safe environment for himself. In general, our teenager participants selected who they talk with and chose to engage with people who are respectful and not prone to use rude or offensive language.

Many bystanders and parents in our study agreed that teenagers' safety should be the top priority. Yet, as adult users, bystanders and parents often focused more on engaging in interesting conversations when they themselves were users.

Seeking peers from the same age group. Furthermore, nearly all teenagers preferred to interact with a certain age group in social VR. as most teenagers often felt a greater sense of safety and comfort in forming friendships with users of the same age due to their shared experiences, common interests, and mutual

understanding that come with being at a similar developmental stage.

> "*I feel like it's just easier to talk to my age. Because they just usually play for fun portion and then the older group I feel like it's just harder to talk to. Because they're just not the same age, so they can't relate to the things I do.*" – T5 (15, male)

This perspective was further confirmed by many parents and bystander participants. For example, several parents mentioned that it is safer for their kids to interact with their own age group and peers. For example, P19 commented,

> "*I want my kids to kick it with their peers in virtual reality, keep them safe and happy, by encouraging our children to become friends with individuals who are their own age or who they already know, we can provide them with a greater sense of security and comfort in these virtual environments.*" – P19 (37, female)

In this quote, she emphasized the importance of parental involvement in keeping children safe and happy in social VR and she suggested that parents encourage their children to form friendships with individuals who are of their own age. By doing so, children could establish clear boundaries for communication and minimize the potential risks associated with strangers interacting online. However, It should be noted, that judging a user's age through their avatar is very challenging, as in most cases, there is no reliable indicator of a user's age in their avatar. A user's voice can be a reference, although mistakes can still occur. We will further unpack this point in the discussion.

Migration to cross-platforms to extend friendship. As social VR remains a synchronous platform, maintaining relationships becomes more difficult if the other users were not online. Thus, among many teenager participants, it was very common to migrate their interaction from social VR to other platforms (e.g., Discord), as they believed Discord offers a more convenient way to communicate with friends and sustain their relationships outside of the virtual environment. Furthermore, Discord's features to allow users to hide their identity and personal information, as well as the option to block individuals who make them feel uncomfortable or unsafe, provided a sense of control and security that is highly valued by many teenagers. T7 (13, male) commented on his experience with Discord:

> "*I decided to get Discord because it was what my Rec Room friends were using, and I just got it. And then I was like, hey I like this. Now I spend a lot of time talking to my friends about this. I'll never give them my number or email. Because that's, like personal. But Discord, I feel like you can still hide your identity.*" – T7 (13, male)

On the contrary, a few parents believed that using Discord may cause additional risks to teenagers' safety since they believed that teenagers tend to share their personal information more easily on Discord, which could potentially lead to further risks. P20 commented:

> "*I was worried about my kid using Discord. I heard about these predators on the internet that try to get kids to give them their personal information. And I thought, what if my kid gets caught up in that.*" – P20 (41, male)

It is important to highlight that many other parent participants were not aware of the extended communication through these external platforms. This discrepancy made it challenging to maintain teenagers' safety. While most teenagers preferred to use other platforms to continue engaging with the people they met in social VR and believed it would be safe to do so, there was a lack of attention to these platforms from the parent's perspective. We will further discuss this phenomenon in the discussion section.

Casual activities to enhance relationships

Social VR offers a unique and immersive experience that makes many seemingly unlikely social interactions possible in a virtual world. Nearly all teenagers in our study discussed their experiences of many different activities, such as playing games, dancing, sleeping, etc. Among these activities, some teenagers believed that casual activities (e.g., watching movies, having virtual parties, etc.) were effective ways to enhance the relationship among different users.

One popular activity that has been witnessed or experienced by multiple bystanders and parents is virtual drinking. To engage in this activity, one would enter a virtual bar that simulated the experience of a real-life bar, allowing them to socialize and spend time with their friends in a simulated bar environment. Essentially, virtual drinking events inherently serve as a social gathering that facilitates connections among users. However, some of the bystander and parent participants have expressed concerns about the involvement of teenagers in these events, as these drinking events were open to all ages and may nudge teenagers to drink in real life. Even though they have not yet seen such incidents happening to their teenagers, their concerns still exist. For example, P24 (35,

male) stated the appropriateness of the situation, especially in the context of teenagers potentially being exposed to adults getting drunk in social VR:

> "*I see a lot of adults in a lot of the drinking worlds, for example, like the party drinking worlds, a lot of people seem to have a really really hard problem with either alcoholism or addiction [...] I worry about kids, as well, you know, because kids are impressionable, and this game is filled with predators. There are plenty of people who will take advantage of kids while they are drunk, just in general.*" – P24 (35, male)

Furthermore, some parents further commented that those who got drunk in social VR environments may engage in behaviors that would be dangerous or intolerable in the real world, such as harassment, which could be especially harmful to teenagers. They may engage in inappropriate behaviors that could harm or exploit children, such as sharing inappropriate or explicit content or asking for personal information.

Safety measures.

As some teenagers appeared to be aware of the risks of connecting with virtual strangers, they have developed and adopted some measures to ensure their safety.

Use alternative identifications. One safety measure that several teenagers reported employing was being cautious about sharing their personal information. For example, in T1's (17, female) example, her approach of not sharing her name with strangers was an effective way to protect her personal information and maintain distance from individuals she did not know.

> "*I feel like I can trust strangers to a certain level, but I'm not fully trusting. I'm not gonna tell my name. I'll normally just have my friends call me by my first initial when I'm online. That is a common thing.*" – T1 (17, female)

From some parents' perspective, they were concerned that teenagers might not be able to properly manage the distance with strangers and would possibly reveal personal information, which may further lead to great risks. Some parents confirmed such risks when interacting with strangers. P21 (35, male) shared his daughter's experience when she interacted with a stranger (an adult) who tried to communicate with her. In this case, he referred to the stranger as a "predator".

> "*My daughter was in the VRChat and people asked her for her address and if she has Facebook or Instagram. I don't want to judge anything, but at that moment, I thought there may be a pedophile, preying on children. Like what grown men ask like a child for Instagram and addresses just for friendship?*" – P21 (35, male)

Using avatars for anonymity. Most of the social VR platforms provide a variety of avatar options, including humanoid avatar (e.g., AltspaceVR, VRChat, Bigscreen) or non-humanoid avatar like an animal, superhero, or historical figure, or customized avatars from third-party platforms (only supported in VRChat), etc. [251]. This is, for the most part, designed for users to represent themselves in social VR. Some teenager participants agreed that social VR avatars could facilitate friendships by creating a visual representation of users that can be interacted with, allowing for greater immersion, social presence, and connection between users. Additionally, avatars facilitated nonverbal communication, such

as gestures and body language. This is particularly important for conveying emotions, which are an essential aspect of human communication and are often difficult to express through text-based interactions.

Interestingly, using avatars may also create a sense of safety for some teenagers. In our dataset, several teenagers mentioned that avatars could provide people with a degree of anonymity and allow them to express themselves freely without revealing their real identities. This sense of anonymity made them feel more comfortable and less self-conscious, enabling them to build relationships with others more easily. As T1 (17, female) mentioned, using avatars made her feel safer:

> "*I feel safer because it's not really a high risk. You don't really know who I am, you don't know where I live. You don't know what it looks like, it just feels safer having those cool avatars to represent you!*" – T1 (17, female)

3.4.3 Teenagers' safety threats

Prior work has suggested various types of threats in social VR, such as sexualized language, hate speech, visible sexual gestures, and so on [35, 81]. We continue to explore the safety threats that teenagers may face. In particular, our multi-stakeholder approach allowed us to explore not only teenagers' experiences but also the observed incidents from bystanders' and parents' perspectives. As a result, some of the following threats were reported by teenagers directly while others were observed by either bystanders or parents.

Sexual harassment through erotic role-playing.

Erotic Role-Play, or ERP, is a type of role-playing activity performed mostly or exclusively for sexual behavior and intentions. To do this, users would customize their avatars and decorate their avatars with symbols or components that have a sexual connotation.

Our teenager participants did not report their own experiences with ERP. However, some bystanders and parents repeatedly reported examples of ERP based on their experiences and how teenagers were engaged in ERP-related activities in social VR. They raised concerns about teenagers' access to adult-only ERP chats and content, such as virtual sex, lap dancing, etc. These activities were designed only for adults and would need to be accessed through private links on external channels (e.g., on Discord). However, these external channels were not associated with social VR applications and thus, were not restricted by the policies on social VR apps. As a result, teenagers were able to access such content easily.

For example, B11 (21, male) shared that while ERP activities were not published in public rooms, teenagers could still access them through quick searches in Discord channels or similar platforms, after which they would then ask for an invitation. He shared the time when he learned a teenager who got involved in ERP from a report :

> "*I follow some reports. I think he was just a 15-year-old who reached out to someone who did ERP [through Discord], and he released his age to the person in the ERP but still went through it. They allowed him to have some sort of ERP, even knowing his age.*" – B11 (21, male)

Another example further suggested an alarming fact that even though the harassment activities happened in social VR, they started from places other than social VR. The safety measures and policies in the social VR platforms, regardless of their effectiveness, did not cover these external spaces, which may cause invisible threats to teenagers. Another bystander commented on this point:

> "*I think that it's accessible because it's as easy as a click of a button. If a teenager found out that there's a community for ERP or lap dancing, they could join the discord and figure out how to get in or something.*" – B12 (22, female)

Relatedly, to enable erotic role-playing (ERP), one would need to have customized avatars through third-party platforms/software (e.g., Blender, Unity), and then import their avatars to social VR platforms (e.g., VRChat). Users are not obligated to adhere to any specific rules regarding the appearance of their personalized avatar on third-party software unless they need to meet certain technical requirements (e.g., rigging, polycount, textures, materials, and model format). Thus they are free to use any design, such as sexual components, insulting language, etc. These avatars may be inappropriate for teenagers to be exposed to.

"Feel" virtual harassment through phantom sense.

Phantom sense is a phenomenon caused by immersion in a VR environment where a user's brain tricks their physical body into feeling touch sensations on their virtual body in virtual environments. This phenomenon arises from the mind's confusion between reality and the virtual world. For example, when a

user gets close to a fire in VR, their body will feel the heat. Usually, users can trick their minds to believe it is real and gain the ability to actually "feel" things in VR. Generally, there are different types of phantom senses - touch, smell, warmth, pain, etc., and every user can feel them, but some are more susceptible than others. It should be noted that with proper training, a user can make their phantom sense stronger and start feeling things and objects inside virtual reality.

While phantom sense can be used to intensify the emotion and joy of social VR activities, it may be misused by some malicious users for their own advantage. In our study, some teenager and bystander participants reported their experience of being harassed through phantom sense. T8 (17, female) shared her example:

> "*I have phantom sense on my arm, forehead, and nose too. It's not good to have it though. I regret mentioning I had it. If people know about it, a lot of them will abuse me. It feels like someone is scratching me, it's itchy ... I took off my headset like it makes me feel uncomfortable when they get close.*"
> – T8 (17, female)

Relatedly, a few bystander participants reported an alarming fact: they reported that some teenagers took advantage of phantom sense and harassed other users without knowing the real consequences of it. For example, B10 (20, female) observed that when a female user talked about her phantom sense, a few other teenage boys in Rec Room started to touch her body. This particular incident becomes alarming since teenagers, without proper guidance and rules in social VR, may flip their role from victims to predators without realizing it. She explained:

> "*I know quite a few people whose phantom sense becomes second nature to them to feel the things that they see happening to them. And don't ever say*

that you have phantom sense, because teenagers will do things to you against your will. I've seen it happen so many times in Rec Room that someone's talking about her phantom sense and as soon as you hear that everyone flocks to that person trying to find out who has it. They start touching her boobs, they start trying to rub her down there. They try kissing her or touching her neck." – B10 (20, female)

In B10's example, she highlighted that teenagers may not have the maturity to regulate their behaviors in social VR, which could cause a risk for others who have a phantom sense to feel hurt in the physical world.

Physical aggression.

Virtual physical aggression. Physical aggression is behavior causing or threatening physical harm toward others. It includes hitting, kicking, biting, using weapons, and breaking toys or other possessions [66]. In our study, some teenagers reported various cases in which they were involved in physical aggression. For example, T5 (15, male) explained his experience with a team-based game in social VR:

"*It's a team-based game where four people versus the other four people and I'm on one team and I kill one of their teammates, and the teammate starts being toxic and stuff, and the whole team just targets me, and hits my avatar, only because I killed their teammate.*" – T5 (15, male)

In this case, neither our participant nor the other players in the game were physically hurt. However, the experience that our participant went through

was disturbing. Such incidents became even more concerning considering the interconnection between physical aggression and violent behaviors, as research has shown that exposure to violent VR content could lead to elevated levels of aggression [195], posing long-term impacts on teenagers' mental health.

Parents normalize physical aggression. Interestingly, some parent participants held a different opinion regarding such physical aggression. They seemed to have normalized physical aggression and considered it as a normal aspect of playing virtual games. For example, P22 (45, male) mentioned that such behavior should be accepted as part of the gaming experience.

> "*So far, the only thing they [my kids] told me is that their thought on somebody who destroyed their house in Minecraft. Stuff like that happens in gaming. So somebody beat them in a game all the time and they were angry, but that's normal.* " – P22 (45, male)

P22 later suggested that he was also aware of the potential negative impacts of aggression and was taking steps to address it by asking his kids to share their experiences with him. As researchers, we believe that more active actions are needed to stop aggression from happening, as exposure to aggression in video games can have negative effects on children's behavior and social development [13]. We will further unpack this point in the discussion section.

Virtual grooming using avatars.

Grooming is one particular type of threat that can be difficult to identify by teenagers, as they are typically the victims without realizing it. Grooming refers

to the situation in which an adult manipulates or abuses children or teenagers through building relationships and trust [69, 144, 169]. In our study, some bystanders shared their observations which they considered as grooming. For example, B10 (20, female) shared an example in which she unsuccessfully tried to help a 6-year-old boy.

> "*[PlayerID] admitted that he was looking for younger girls to be friends with, and he was 35. He had this 6-year-old, eating out of his hand. He groomed her into thinking that he was her friend and that she could only trust him, and I tried to help her. I tried to tell her this guy is a predator but she didn't believe me, she was too far gone.*" – B10 (20, female)

This was an alarming example. Existing social VR platforms generally have a suggested age limit for their users (e.g., the age requirement for VRChat is 13 years or older [3]). Yet, children younger than 13 still accounted for a large percentage of the user base. Thus, users with malicious intentions may easily take advantage of them through grooming. Furthermore, avatars hide the real identity of the people behind them, making it difficult to identify the adults and their intention. As a result, trust can be built through some innovative ways, such as using a child's favorite avatar. P18 provided an example:

> "*I just feel in a virtual reality setting, kids are more susceptible to manipulation. You can make that avatar something similar to a character that the younger kids would love. I would expect that to happen in VR, and any form of that, I would consider abuse and manipulation.*" – P18 (29, female)

Potential threats in a private room.

In social VR, users can create or join private rooms, which are invitation-only spaces. The purpose of these private rooms is to provide a more controlled environment for users to interact and engage in activities. To understand the dynamics in private rooms, it is necessary to talk to people who have experiences in these rooms. In our study, several teenagers, parents, and bystanders have been invited to join private rooms, and their experiences pointed to potential threats to teenagers' safety. For example, P23 (53, male) shared a case in which teenagers were invited to watch adult content in a private room in Bigscreen (a social VR app that supports movie sharing) and faced unforeseeable risks:

> "*I've seen it [adult content] quite a few times on Bigscreen. Adults will ask a child to join them in a private room and send a link to it. Or they'll open a room, then make it private when you're in there [...] I've seen porn movies in open rooms in Bigscreen. They're supposed to be safe so children don't see them. But they're not.*" – P23 (53, male)

When facing threats in private rooms, some teenagers were able to identify, then responded proactively to combat the threats. For instance, T5 (15, male) witnessed a situation in which an adult user tried to lure a teenager into a private room in Echo VR. He quickly recognized the threat and took immediate action by reporting this adult user:

> "*I was chatting with a guy in Echo VR and an older man teleported in and talked to another player who was a boy. When I got closer to them, the older guy went quiet, he was trying to take the young kid to the private lobby to keep talking to him after I confronted him, I reported him.*" – T5 (15, male)

As suggested by these examples, in private rooms, teenagers' threats and possible mitigation strategies may not be obvious to users and remain ineffective. We will discuss the implications in the discussion section.

Ability-based discrimination.

Occasionally, the social VR environment was lacking inclusiveness, as reported by our participants. A few teenagers reported that they have witnessed incidents in which other users discriminated against some teenagers with disabilities.

They highlighted the possibility that those users may not recognize the challenges that teenagers with disabilities may experience in social VR, and their seemingly joking behaviors may lead to discrimination, which negatively impacted the experiences of teenagers with disabilities. For example, a teenager described an incident in which another teenager with a speech disorder was discriminated against by other users:

> "*I've seen a kid that had speech disorders or speaking disabilities, he did speak weirdly, like he did not spell some word properly and they would go up to him and would make fun of him and ask why he has it.*" – T7 (13, male)

3.4.4 Desired safety features in social VR

Similar to previous studies that have focused on marginalized users (e.g., members of the LGBTQ community or women) who have used nonverbal communication (e.g., specific gestures) to protect themselves from potential harassment, [151, 185], our study explored several safety practices commonly used by

our participants, such as reporting to the platforms, banning/muting/blocking other users, making other users invisible (e.g., using Personal Space Bubble), and assessing other users' trustworthiness before interacting with them (e.g., through Trust Rank). In this section, we present some nuances regarding participants' desired safety features.

Age matching mechanism. Many teenagers and bystanders often preferred to interact with others from a similar age group, while some parents preferred their teenagers to do the same. Our participants believe that matching players in public games based on their age may have a very positive impact on the social VR community by reducing undesired safety risks and harassment. As a teenager illustrated:

> "*I would probably try to separate it, like having two dedicated games, one for children and then one for adults. I think that would help mitigate harassment or even make it even easier to track who's harassing who and maybe make the discipline.*" – T6 (13, male)

This age matching system was one of the most favored safety features by the majority of participants, yet it is important to acknowledge that implementing such features could inadvertently provide opportunities for predators. For example, predators could potentially exploit the system by reporting to be a kid, gaining approval from the platform, and then accessing a kid-only environment.

Age verification. To facilitate the age-matching process, another relevant safety feature is age verification. Some participants were looking for a feature in social VR platforms to ensure that a predator could not fake their age to access children's

rooms and vice versa. For example, P24 (35, male) suggested that the platforms should ask for photo ID to confirm the identity and the age of the users:

> "*I'm hoping for a way to verify your age. So like a passport or something to verify that you're actually over the age of 13, so that minors don't get targeted by older audiences. I feel like kids should play with other kids and then everybody should play with their own age group.*" – P24 (35, male)

Sexual harassment history indicator. As mentioned above, a banned user may create a new account and continue using the service. One safety feature that could remediate this issue would be to have an indicator on users' avatars regarding their harassment history. For example, P23 (53, male) suggested that the avatar of a previously banned user may include an indicator (e.g., a badge) to show their prior harassment record in the platform as a warning to other users:

> "*I feel like those who have been banned for sexual assault, or sexual behavior in a public area, should have some kind of mark on them [their avatars]. Like a sexual predator predictor. I feel like that would definitely help the community and maybe even discourage sexual assault.*" – P23 (53, male)

This feature was highlighted by a few participants as a potential strategy to identify predators. While it may initially appear to be a promising approach, it is crucial to recognize that its implementation could inadvertently raise new forms of harassment within the platform. For instance, users may specifically target or launch attacks against individuals who display this indicator, resulting in unpredictable consequences.

Parental control and involvement. Some participants highlighted that a significant part of child safety lies with their parents. Thus, some participants recognized the importance of having parental controls, such as limiting children's playing time, limiting the number of social VR platforms used by their children, etc. Our participants also suggested that parents need to be more engaged in their children's activities and be aware of the people they socialize with in social VR.

3.5 Discussion

As we move into an increasingly digital world, the realm of virtual reality (VR) has become an important area of focus for Human-Computer Interaction (HCI) studies. The rise of social VR presents new and unique challenges, particularly regarding the potential risks associated with its use. While previous HCI studies have explored these risks, it has been noted that most of these studies have only focused on a single group of users, such as young adults or bystanders [35, 81, 208].

Our study endeavors to explore teenagers' social VR experiences from the perspectives of teenagers, bystanders, and parents, who are all essential stakeholders in social VR ecosystems.

This multi-stakeholder approach takes advantage of the unique experiences and perspectives of each stakeholder and provides different yet complementary angles to understand teenagers' experiences and identify potential threats in social VR.

Our results revealed a number of threats that teenagers may face in social VR. Some of the threats came from teenagers' experiences while others were observed by bystanders and parents. In this section, we reflect on our findings and further discuss how these findings shed light on nuanced forms of threats and social norms. Based on these findings, we also discuss the implications of designing safe and healthy social VR platforms as safe spaces.

3.5.1 Categorizing the sources of teenagers' safety threats

Our results suggested different types of safety threats that teenagers may face in social VR. Upon further examining these threats, we started to note the causes of these threats and grouped them into the following categories.

Discrepancies among the perceptions and experiences of teenagers, bystanders, and parents. Our data suggested teenagers, bystanders, and parents constantly held different opinions and/or experiences towards the same activities. Such mismatch may have led to some hidden threats which may not be obvious otherwise. For example, in the case of building connections with strangers in social VR, most of our teenager participants have normalized this action to be a fundamental aspect of social VR, yet parents and bystanders pointed out cases in which teenagers may face privacy and security risks due to the interaction with strangers. In the example of virtual grooming, our teenager participant built trust with the predator easily, yet bystanders who observed the situation tried to help the teenager but were refused, leading to greater risks of being harassed by the predator. In the example of physical aggression, our teenager participant who experienced physical aggression had disturbing feel-

ings, yet their parent believed that it was an integral part of the game experience in social VR. When these discrepancies exist, teenagers would either not accept the help offered by others (since they believed that risks did not exist) or not ask for help when needed (since other stakeholders may not care about it). It became difficult to convince others to take proactive action and mitigate the potential risks.

Lack of social norms in social VR. Social norms, behaviors, and values in the physical world are shaped by socialization processes, cultural contexts, laws and policies, and broadly-acknowledged values.

Similar to our physical world, social VR also represents a complicated social space that includes different types of users, events, and activities. Yet, the norms in our physical world may not necessarily translate to social VR environments. In fact, social VR did not seem to have established social norms that users follow to maintain a proper environment. For example, in the case of drinking alcohol in a bar, teenagers would not have access to an actual bar due to the age restriction. Yet, the lack of social norms in social VR made it possible for them to access the virtual bar and participate in activities, some of which might be inappropriate for teenagers (e.g., some teenagers were nudged to drink alcohol in real life). In the case of ERP, teenagers may also be exposed to sexual content (e.g., avatars with sexual symbols or signifies), which was against the established social norms in the physical world yet remained popular in social VR.

We consider these types of threats as "hidden threats", which could be easily overlooked otherwise.

A challenge in identifying and defining social norms within social VR lies

in its inherent anonymity. When users embody themselves through avatars, specific identity information (e.g., gender, age, and preferences) may be lost. However, the norms users are used to in the physical world are largely based on users' identity, and thus, are no longer effective in social VR. Future work should investigate human behaviors in social VR and help establish/identify appropriate social norms to ensure a healthy VR environment for teenagers.

Technological limitations and barriers. As social VR is evolving and not sufficiently mature, it also creates some technical limitations for users. For instance, moderators play an essential role in social VR, particularly in case users need help. However, moderators were not readily available in private rooms where safety threats were quite common. Instead, the responsibility of moderation is often left to the owner or creator of the private room who may not have the experience to effectively manage the dynamic of the environment. As a result, these private rooms can inadvertently become safe havens for predators to engage in harmful activities, such as grooming, bullying, or exploitation of teenagers.

Additionally, VR devices also introduce limitations by providing an enclosed first-person experience only to the user. As such, our parent participants generally lacked participation in their children's VR activities. In fact, only a few parents in our study stated that they regularly played in VR with their children. Currently, social VR platforms do not support ad-hoc recording or checking history functions, making it difficult for teenagers to document their experiences and for parents to learn about these incidents. As such, this limitation further deepens the perception gap between teenagers and parents and may potentially cause more harm in the long run.

Finally, the immaturity of social VR ecosystems also contributes to teenagers' safety threats. For example, the process of avatar creation and customization also introduced further limitations. In our study, participants who wanted to customize their avatars needed to turn to third-party software or platforms (e.g., Unity, Blender). However, those platforms did not have proper guidelines or validation mechanisms to regulate the process. Social VR platforms also did not have power over these third-party platforms nor provided mechanisms to filter customized avatars other than some technical limitations (e.g., customized avatars cannot exceed certain sizes). As a result, users can freely create and utilize avatars to meet their individual needs which could potentially turn their avatars into vehicles of harassment (e.g., ERP).

3.5.2 Design implications

Designing age-specific matching mechanisms for social VR. We propose the implementation of an age-matching system for social VR platforms, considering the significant usage of these platforms by teenagers and children. As highlighted in section 4.4, our participants expressed a strong preference for interacting with peers of a similar age. While some platforms offer junior accounts, the existing age verification system falls short of ensuring the accuracy of users' real age. We suggest that platforms consider implementing parental consent as a means of age verification. For instance, during the account creation process, the platform could send a link to the parents' phone that when clicked can allow them to sign a consent form. Moreover, while we acknowledge the possibility of users attempting to fake their age, additional ongoing monitoring measures can be put in place. These monitoring measures could involve the use of algorithms

to detect suspicious behavior or inconsistencies in user profiles such as being reported multiple times or sending many unnecessary messages. By flagging potential discrepancies or anomalies in user activity, the platform can prompt further verification checks to ensure the accuracy of the user's age information.

Enable recording in social VR. We believe that it would be beneficial to incorporate a feature that allows users to share evidence with social VR moderators in case of unsafe and/or uncomfortable experiences. We propose the implementation of an "emergency button," similar to the screen recording functionality in the Zoom video conferencing software, to assist teenagers to request help when experiencing harassment, aggression, or other unsafe incidents in social VR. Activating this button would initiate the automatic audio and video recording of all activities within the user's vicinity, providing valuable evidence for future reference. It should be noted that to avoid abusing such a feature, the recorded media must be securely stored (ideally locally in VR headsets) by the social VR platforms and should be made exclusively accessible to the system moderators who can review them and take appropriate actions. Furthermore, the platforms should promptly notify moderators and parents when a user uses this feature to ensure their well-being.

Supporting non-tech-savvy parents and guiding children's social VR Experiences. Concerns over the safety of teenagers in social VR have prompted many parents to seek further education in this field given their limited familiarity with the platform. To this end, one effective approach to address this need would involve updating existing safety education resources to include a dedicated VR component highlighting the potential risks and threats. Such materials could help raise awareness of harassment and sexual abuse issues in social VR among

parents and their children and the same time equip children with the necessary knowledge to safely use social VR.

3.6 Conclusion

Social VR platforms have become increasingly popular in recent years among teenagers, yet safety issues such as harassment and sexual abuse continue to be significant concerns. This paper aims to investigate teenagers' experiences in social VR through three different perspectives, with a specific focus on harassment issues. Through an interview study with 8 teenagers, 9 bystanders, and 7 parents, we identified several threats for teenagers in social VR, including grooming and manipulation in private worlds. We also highlight new forms of harassment in social VR, such as Erotic Role-Playing and through phantom sense. Our findings provide a better understanding of the risks faced by teenagers in social VR and offer insights to design safer and more fulfilling experiences for them. We hope that our study contributes to the ongoing efforts to create safer social VR environments for teenagers.

3.7 Acknowledgment

We thank the anonymous reviewers and the shepherd for their invaluable feedback. We also thank our participants for sharing their insights. This work is partially supported by a research gift from Meta.

CHAPTER 4

HELP-SEEKING BEHAVIOR OF YOUTH NAVIGATING THE DIGITAL-SAFETY ECOSYSTEM

4.1 Introduction

Digital abuse affecting youth constitutes a public health issue with serious and potentially long-lasting psychological and physical repercussions. Despite this risk, help-seeking resources for digital abuse remain underdeveloped compared to resources for mental health contexts, and there is limited understanding of how youth engage or fail to engage with help-seeking pathways in response to digital risks and harms. In this work, we explore the help-seeking behaviors of youth (10-17 years of age) in response to digital abuse, the events that precipitate help-seeking, the support systems that youth engage in, as well as factors or obstacles in their immediate environment that influence their willingness to engage with support systems.

Digital technology provides youth continual opportunities for learning, communication, and self-expression [133, 129]. As youth increasingly access digital devices and services, they are more exposed to digital risks and harms such as cyberbullying and harassment [118, 78, 15], inappropriate content [78, 178, 226], sextortion [74, 9], and financial fraud [78, 138]. The ability of youth to navigate these challenges and seek help when necessary is crucial to their well-being and healthy development [174, 236, 231]. Therefore, understanding youth help-seeking behavior or inaction in response to digital threats and harms is essential for designing effective interventions, policies, and educational programs that promote digital safety and resilience.

Prior research described that youth recognize gaps in their knowledge to understanding and mitigating online threats while at the same time noting that there is a lack of available resources to obtain this knowledge [78]. Moreover, youth are not included in the development and design of safety measures, such as content monitoring or restricting apps, which leads them to perceive adults' protective efforts as intrusive and infringing on their autonomy. This can result in a lack of acceptance and lead them to circumvent these protective measures [78, 5]. This paper contributes to a growing body of research dedicated to understanding the complexities of the digital-safety landscape [180, 213, 78] and challenges of help-seeking [106, 46], as well as research promoting youth well-being through help-seeking, resilience, and digital safety interventions [5, 52, 61, 128]. To effectively design online safety strategies for youth and the stakeholders that support them, it is important to understand how they seek help when encountering digital threats.

In this paper, we describe the sociotechnical complexity inherent in the help-seeking ecosystem and how youth navigate their help-seeking journeys amidst this complexity of virtual and nonvirtual abuse experiences. We define the help-seeking ecosystem as an interconnected system of individuals, professionals, organizations, and resources in the physical and digital world that collectively provide assistance to someone in need, focusing on how different types of resources coordinate or clash with each other and are embedded in the intricate fabric of social connections and relationships. By drawing on perspectives and lived experiences of adolescents and adults who are part of this help-seeking ecosystem (parents, teachers, mental health professionals, advocates, physicians, and lawyers), we analyze help-seeking resources and behaviors in relation to a wide spectrum of attackers, threats, and harms that span platforms and the digi-

tal and physical realms. To examine these issues and expand the understanding of the challenges faced by youth and stakeholders when seeking help in response to digital abuse experienced by youth, we pose the following research questions:

RQ 1: What are the most common support resources that youth engage with?

RQ 2: How do risk and protective factors in their (youth) immediate environment influence—positively or negatively—their willingness to engage with support systems? How does their help-seeking behavior differ based on the digital harms they encounter?

RQ 3: How can these support systems be improved to better meet youth needs with respect to digital harms?

Our paper makes three main contributions to the human-computer interaction (HCI) and computer security community. First, we advance the understanding of social support seeking in response to digital threats and harms experienced by youth. To date, there has been no multi-stakeholder investigation of how youth seek help in response to digital threats and harms. We fill this gap by contributing a qualitative study that examines youth digital help-seeking from the perspective of multiple stakeholders in response to digital threats. We highlight the fundamental challenges encountered by youth when seeking help in response to digital abuse and the difficulties experienced by adult stakeholders in providing help that aligns with youth experiences. We also account for the potential risks that youth face post-reporting, illuminating the need for ongoing support from both technology companies and the mechanisms of security and privacy protections available to them.

Second, building on ecological support approach [233] and communal coping model [143], we contribute the PROTECT framework for Youth Digital Safety (**P**roblem recognition, **R**eaching out, **O**rganizing support, **T**raining in digital literacy, **E**ngaging professionals, **C**ontinous support, **T**ackling safety measures) which accounts for an overall help-seeking ecosystem, rather than help-seeking on a single platform or from a particular support source, in order to untangle the social and contextual dynamics of help-seeking behaviors, the dynamic interplay of different support resources, and their relationship to different types of digital risks and harms. Our study expands the boundaries of ecological and communal coping theories to accommodate digital abuse situations. Finally, this study points out the need to ensure that responses to digital abuse align with the needs of the affected youth. We emphasize that it is important to focus on providing timely and trauma-informed support to these youth, effectively addressing their concerns. A trauma-informed approach recognizes the ubiquitous impact of trauma on individuals and emphasizes a holistic path to include trauma-sensitive or trauma-responsive services [1, 2].

4.2 Related Work

We begin this section by laying out the complex sociotechnical landscape of youth digital risks and harms. We then describe youth help-seeking in mental health as this is the most studied area of youth help-seeking. We then describe the understudied area of help-seeking in response to digital abuse. We follow with a discussion of conceptual models and conclude by describing our work through the lens of ecological and communal coping theories.

4.2.1 A complicated landscape of digital risks and harms

As technology use has become an integral part of teenagers' lives, it is also being used as a tool of abuse in teenagers' interpersonal relationships [215, 240]. Protecting youth from digital risks and harms has been identified as a critical issue [20, 131]. Their pervasive interaction with various forms of media and known and unknown individuals has led to concerns about their vulnerability to threats, including unsolicited content, sexual violence, online harassment, cyberbullying, financial fraud, and misinformation. Prior work has explored the nuanced nature of online threats experienced by youth and the protective practices employed by both youth and adults and has emphasized the need for improved collaboration and communication among adults supporting youth [78, 138, 171]. The impact of digital abuse on youth well-being has become a significant concern as it can affect mental health and well-being, including increased risk of depression, anxiety, self-harm, and suicidal ideation [101, 175, 188, 64].

A recent study on youth digital safety described how abusers could be peers, strangers, or anonymous individuals, making the abuse feel unavoidable and omnipresent [78]. The ephemeral and ubiquitous nature of digital spaces, the relative anonymity of perpetrators, and the rapidly evolving forms of digital abuse can create barriers to identifying, reporting, and mitigating abuse [78, 57, 99]. The harms and threats that youth experience and their need for support are incredibly diverse and, as such, there is a need to understand how all of these factors can influence help-seeking.

4.2.2 Help-seeking behavior in mental health contexts

The most well-studied area on the help-seeking behavior of youth has been conducted within the context of mental health [139]. Mental health help-seeking has been characterized as an adaptive coping process; that is, the attempt to obtain external assistance to deal with a mental health concern [194].

Youth who deal with mental health issues are often reluctant to seek help from formal sources, leading them to internalize blame and experience shame [55, 98]. However, they engage in a variety of other coping strategies, for example, by venting to and seeking support from peers, blocking upsetting content, unfollowing problematic individuals, and building support systems through online connections and communities [139]. The barriers to help-seeking are youths' misunderstanding of digital abuse and risks, perceived lack of understanding in adults, lack of trust in support resources, fear of consequences, not wanting to burden or disappoint their families, and perceived pain from dealing with emotionally disturbing situations [139].

Offline approaches to help-seeking, such as reaching out to health professionals or confiding in family and friends, have been shown to have inherent challenges. Stigma and concerns about societal perceptions associated with mental health issues may deter individuals from seeking help due to fear of judgment or discrimination [55, 204]. Moreover, cultural and personal inclinations towards autonomy frequently dissuade youth from seeking support from their peers, even in instances of mental health challenges [193, 87]. This desire to handle one's own problems can exacerbate feelings of isolation and mental health distress.

Beyond offline options (e.g., mental health professionals), there are mental health websites and forums, as well as broader social media platforms that allow for anonymity and control and that can alleviate many barriers associated with help-seeking online [113, 201]. This anonymity can reduce the fear of stigma as these platforms offer users the potential to share their experiences without disclosing their real-world identities [26, 12, 51]. Youth also have an array of digital platforms on which to share their challenges, including those that target mental health issues [125, 124, 121, 126, 123] and those that provide broader options for sharing content that include mental health posts (e.g., Instagram, TikTok) [29, 155, 184].

Prior work examined how asynchronous remote communities support mental health interventions among young people. Yarosh et al., (2017) showed that online platforms often supplement traditional mental health services by offering a sense of community and peer support, which is crucial for the help-seeking process [249]. In the context of self-injury support solicitations and responses on a mobile peer support app, a mixed-method study by Kruzan et al. (2021) identified the prevalence of indirect solicitations to mitigate stigmatization concerns, as well as a higher frequency of emotional support seeking over informational and other types of support solicitations [122]. The indirect solicitations were identified as effective entry points for conversations that mitigate threats, especially for stigmatized conditions [122, 45].

Additional research investigated the role of social media-based mental health support among college students exploring how social media platforms can provide a valuable avenue for mental health support highlighting the importance of online communities in facilitating connections and sharing experiences [238].

This research highlights the importance of help-seeking for mental health support for youth as digital applications can play a role in fostering a sense of community and peer support, which is essential for the mental health help-seeking process.

However, while online support can offer an avenue to facilitate conversations, these apps or communities can sometimes inadvertently have negative consequences. For example, in some online communities, peer support exchanges can contribute to enabling negative support [88] by reinforcing and validating maladaptive behaviors (e.g., eating disorders) [50, 221]. This highlights the complexity of the help-seeking process in mental health contexts and raises the importance of providing support that aligns with the help-seeking needs of youth. Additionally, it calls for protective measures to ensure that the very tools and communities providing support to vulnerable youth do not perpetuate harm. From this perspective, it becomes important to understand and describe the multidimensional landscape of digital abuse and how youth seek help in response to these digital risks and threats.

4.2.3 Help-seeking for digital risks and threats

In the context of digital abuse, the dynamics of help-seeking behavior can differ markedly from those relating to general mental health issues, which calls for understanding both enablers and barriers to help-seeking, as well as how they vary for different types of digital harms and contexts in which youth encounter them online. Considering the range of circumstances in which digital abuse occurs, and the relationship and physical proximity to the perpetrator, youths' ability to cope and to engage with support systems, both in the physical and

digital worlds, vary [78, 213]

Moreover, digital abuse often occurs within a sociotechnical system with its own set of norms and expectations. By contrast, the mental health system, while often complex and potentially intimidating, provides a structured path for seeking help [32]. There are recognized health professionals, established treatment methods, and prescribed protocols for reporting and intervention. Yet despite these structured processes, youth often encounter barriers that include lack of knowledge about mental health issues, and limited access to mental health resources that can hinder their help-seeking behavior.

Previous research has identified significant barriers to digital help-seeking for digital abuse, including stigma and self-reliance [132]. A study by Barlin´ska, Szuster, and Wisniewski [27] reported that victims of cyberbullying often refrain from seeking help due to perceived stigma and fear of retaliation. It was also found that the anonymous nature of the internet often intensifies the fear of not being believed [132].

The reluctance of youth victims to report digital abuse is often compounded by the belief that adults may not understand the digital context or respond appropriately [75]. A 2010 study by Nocentini et al. expanded on this issue, demonstrating that adolescents were less likely to seek help for cyberbullying when they perceived their parents to have low digital literacy [170]. This emphasized the importance of parental digital literacy in encouraging open communication about online harm. Hinduja and Patchin underscored the role of the school environment in shaping students' willingness to report cyberbullying [101]. They found that students are more likely to disclose their experiences in schools that fostered a supportive and inclusive environment, highlighting the

importance of supportive proximal environments in seeking help and mitigating the impacts of digital abuse [101].

Although scholars have recognized the multifaceted nature of adolescent online risk exposure, there is still a considerable gap in the literature regarding help-seeking behavior given the unique vulnerabilities of different youth populations across diverse environments, and in response to various digital threats. Prior research has primarily focused on isolated help-seeking behaviors on individual platforms or venues, rather than providing a panoramic view on help-seeking[189, 244]. However, youth experience a broad range of digital risks and threats across multiple platforms and need support from multiple stakeholders including parents, educators, and advocates. Scholars have also acknowledged the need to further investigate youth online risk exposure to develop effective strategies to safeguard youth in the digital world [19, 36, 93, 241, 198, 244, 77, 242]. These studies have included a discourse analysis emphasizing the critical role of parental trust, control, or involvement [93], as well as design frameworks aimed at parental intervention in adolescent smartphone use [117]. It is critical to consider the sociotechnical complexities in the context of youth's interpersonal relationships and the risks that surface both in the digital and physical worlds.

Continuous access to the internet offers youth the opportunity to foster new and existing relationships and explore their identities through intimate relationships. However, it also exposes them to sexual risks due to the consensual sharing of intimate content that can be later distributed as non-consensual intimate images [206, 250, 228, 78]. Notably, a study found that sexting was the most prevalent form of sexual interaction for which teenagers sought support, with 66% of related posts seeking assistance regarding sexual messages, nude

photographs, or videos, highlighting the need for spaces that facilitate honest and safe conversations among teenagers, both online and offline [189]

There is also a limited understanding of how youth utilize social media as a vehicle to find support [90]. Prior research has explored Instagram Direct Messages as a medium for peer support among youth, specifically concerning mental health and personal issues [106]. Additional research contributes to our understanding of online peer support in the context of sexuality and relationships. Prior research has documented youth's use of Facebook as a platform for gaining social support, and a series of studies have shed light on youth's search for support via publicly accessible content revolving around sexual experiences [189, 106]. Harikainen et al. explored peer-to-peer informational and emotional support in an online youth forum, highlighting the emergence of self-organized norms for handling negative online sexual experiences [94]. Another study underscores the growing digital influence on adolescents' friendships and sexual identity explorations, raising concern about the difficulties they face in rejecting solicitations for nude images from known individuals [95]. These studies collectively underscore the need for further research to understand youth help-seeking to improve youth digital safety.

Closest to our work, Pereira et al. explores help-seeking behaviors in the context cyber-harassment victimization [180]. This survey of adolescents aged 12-16 in Portugal has shown that less than half of them sought help, but the majority of help-seekers preferred to utilize informal resources, which were rated effective in terms of helpfulness; formal resources, on the other hand, were used in less than 7% of all help-seeking cases [180]. In the case of cyber-harassment, informal help-seeking has been identified as the most common coping strategy

used by adolescents who often turn to informal sources or marshal emotional support from others online, known as internet-coping strategy [180]. Youth prefer informal (e.g., relatives and friends) to formal support resources (e.g., mental health professionals, teachers, counselors, police, and support services) for online risks and online harassment [153]. This research, which focuses only on one group of stakeholders (youth), found that victimization mostly occurred within close and frequently encountered relationships, including friends.

Furthermore, according to Pereira et al.'s (2016) study, formal sources were never used alone, with adolescents combining formal and informal resources, which raises questions about pathways through which informal and formal resources of support get activated and integrated with each other. Among reasons why formal resources are underutilized by adolescents are feelings of shame, stigma, fear of retaliation, lack of adequate professional help or awareness of the available resources, and, finally, not viewing them as being particularly helpful [180]. This calls for further exploration into the processes by which informal and formal resources are activated and interconnected.

Evaluation of formal resources as not being helpful aligns with findings from a Pew Research survey showing that adolescents are critical of how online harassment has been handled by teachers, social media companies, and politicians, seeing them as failing to effectively tackle the issue [15], which further highlights the need to investigate how to improve support systems to meet the needs of adolescents encountering digital risks.

Beyond this prior research, there is a need for an in-depth examination of help-seeking landscape to provide perspectives of multiple stakeholders and multiple threats. Our research fills this gap by contributing a qualitative study and

describing the perspectives of youth and the multiple stakeholders that provide support, examining help-seeking behavior of youth in response to different threats [78] and across different platforms taking into account how abuse can span the digital and physical worlds concurrently.

4.2.4 Conceptualizing help-seeking

There are several help-seeking theories and frameworks important for comprehending how, why, and when individuals seek help, and how they find out about resources. Additionally, they can assist in identifying both barriers and facilitators to seeking help, and provide a framework to guide interventions and policies aimed at improving access to provisions of care. We now review four different theoretical approaches that highlight different perspectives to help-seeking: a) Rickwood's help-seeking model emphasizes an individual's health help-seeking journey underlining the importance of individual autonomy in help-seeking particularly in the context of mental health; b) Livingstone's youth skills (ySKILLS) conceptual model focuses on the importance of digital skills in youth's self-development and mental health well-being emphasizing the importance of digital resilience in equipping youth to navigate and recover from online challenges; c) Vaux's ecological theory illuminates the influence of surrounding systems, such as environmental and societal structures, on an individual's help-seeking behaviors; and d) Lyons' communal coping theory introduces the concept of shared problem-solving. In this context, an individual stressor is recognized as a collective issue and addressed through cooperative action. While each model brings its unique perspective, they emphasize the individual's experience but do not focus directly on help-seeking for youth in

the context of digital risk and threats taking into account the broad ecosystem of stakeholders [193, 140, 143, 233]. Our research identifies youth help-seeking in response to digital risks and threats through a multi-stakeholder perspective. By synthesizing perspectives from youth and stakeholders that provide support, we propose the PROTECT framework, which accounts for an overall help-seeking ecosystem.

Conceptual models for help-seeking in mental health contexts

Addressing the mental health needs of young people aged 14-25, Rickwood's model of help-seeking behavior offers a structured approach by which to understand the factors that affect help-seeking among young people [193] and was originally developed within the context of mental health addressing offline help-seeking. Rickwood et al., identified four key stages of help-seeking behavior: awareness, expression, availability, and willingness. These stages are discussed in terms of recognizing one's own distress (awareness), articulating this distress (expression), acknowledging the existence of helpful resources (availability), and finally, deciding to seek help (willingness) [193, 183]. However, there has been limited use of theoretical frameworks to help conceptualize online help-seeking and guide the development of improved resources [183].

Several scholars have applied Rickwood's help-seeking model, which places emphasis on the individual rather than at the structural level, to online mental health help-seeking, identifying it as a valuable framework for understanding the help-seeking process [183, 33]. For example, studies that explore the help-seeking behaviors of young men showed that these individuals were more likely to seek online help due to the confidentiality and anonymity afforded by online

technologies [219, 48]. When viewed in the context of Rickwood's help-seeking model, this willingness to seek help aligned with the expression and availability stages providing a lens by which to view mental help-seeking online and offline [33].

Another conceptual model to help-seeking in mental health contexts takes a different approach by investigating the digital competencies of youth, aged 12 to 17, with mental health vulnerabilities. Using the youth skills (ySKILLS) conceptual model, this work centers around the premise that adolescents are active participants in their development and their digital skills are crucial mediators between the risks and opportunities related to Information and Communication Technology (ICT) use [140]. Livingstone highlights the concept of digital resilience, suggesting that fostering this trait in youth can empower them to effectively cope with online threats. This resilience is crucial for their help-seeking behavior, providing them the ability to identify and respond to digital risks while managing their mental health vulnerabilities.

According to Livingstone, various societal factors such as adult norms, familial expectations, and business policies significantly shape these digital skills. The findings bring into focus the critical role digital skills play for youth confronting mental health challenges, serving not just as self-defensive tools but also as avenues for seeking specialized mental health information [140]. This work also draws attention to the potential insufficiency of even the most advanced digital skills in managing the intricacy of digital services and products. The study examines the specific skills required by individuals with mental health issues, such as coping mechanisms and disclosure skills[140].

Livingstone underscores the heightened risk of these youth due to the indis-

criminate usage of digital skills during certain phases of their life. Her research posits the need for future research to understand how digital assistance can fill the gap left by the existing offline professional mental health services [140]. This works calls for further research to explore how digital assistance can supplement current offline mental health provisions of care. The importance of fostering digital resilience to boost online competences, well-being, and personal agency is also emphasized. Livingstone's work encourages continued collaboration among researchers for more comprehensive data collection and understanding of the intersection between digital skills and mental health vulnerabilities as well as a communal approach to addressing this broad societal need [140]. Furthermore, Livingstone also recognizes the importance of building digital resilience as a means of boosting online competences, well-being, and personal agency among youth. This extends beyond mental health and is relevant to help-seeking behavior of youth in response to digital risks and threats. This strategy can empower young people to confidently navigate the digital world, enabling them to identify, mitigate, and recover from potential online threats, such as cyberbullying and/or exposure to inappropriate content. Livingstone encourages the continuation of collaborative efforts within the research community for better data collection and comprehension of the link between digital skills and mental health vulnerabilities.

Rickwood's help-seeking model can offer insights into the individual mental health factors influencing an individual's decision to seek help, while Livingstone's ySKILLS conceptual model provides a framework for understanding the acquisition, use, and influence of digital skills among youth [193]. While both models are concerned with youth mental health, they approach help-seeking from different, yet complementary perspectives. Rickwood's model is centered

on the help-seeking process. It offers insights into why young people may or may not seek help for mental health issues, and what factors can facilitate or hinder this process [193]. Livingstone's work, conversely, focuses on digital skills and their role in mediating the risks and opportunities of ICT use. It examines how these skills, and the factors that influence them, impact the well-being of young people, particularly those with mental health difficulties [140].

Ecological approach and communal coping

We now discuss the ecological [233] and communal coping [143] models as perspectives that take into account the multi-faceted and holistic nature of help-seeking behavior. By providing a contextual and transactional view on help-seeking, they can advance our understanding of youths' decision-making around how, when, and from whom to seek help in their social ecology when encountering digital harms and risks.

Taking an ecological approach. Vaux's ecological model prioritizes the dynamic transactional process between an individual and their environment [233]. Vaux describes these "networks" as sustainable and able to give support on an ongoing basis. This emphasis is particularly relevant when studying help-seeking behaviors. Rather than looking at these behaviors and the resources they engage with as static components of a person's experience, Vaux suggests focusing on the fluid relationship among appraisal processes, behaviors, and resources [233].

By taking an ecological approach [233], which emphasizes help-seeking as a dynamic transactional process between an individual and environment, and viewing our work through this lens, we seek to understand how youth become

aware, appraise, and choose between different support resources, as well as triggers and deterrents from help-seeking. The social support ecological approach calls for a) mapping the links between appraisals, behaviors, and resources, and b) understanding of personal and ecological factors that shape the help-seeking process [233]. In the context of youth and digital abuse, this perspective illuminates how young people become cognizant of, evaluate, and decide upon the myriad support resources available to them. It also shines a light on what events might encourage or discourage them from seeking support. Rather than treating help-seeking behaviors and resources as static attributes of the individual or environment, we chart the intersections between evaluations, behaviors, and resources, while also understanding how personal and ecological factors shape the help-seeking journey.

Furthermore, Vaux emphasizes the need to map the interactions between these elements and understand the personal and ecological factors that shape the help-seeking process [233]. This may involve examining personal attributes, interpersonal relationships, and broader social and institutional contexts. We view our research through this lens as our research on help-seeking in response to digital abuse not only explores how individuals seek help, but also how their perceptions of their environment and available resources affect this process. Ultimately, Vaux's approach encourages a holistic examination of the complex interactions that determine how, when, and why people seek help. Aligning with Vaux's model, our research examines help-seeking behavior of youth in response to digital threats as a multi-dimensional multi-stakeholder process.

Communal coping perspective. By drawing on Lyons' communal coping model [143], we examine the coordination, or lack thereof, between different support

resources and efforts (e.g., parents, schools, mental health professionals, advocates, etc), and different mechanisms and obstacles for pooling these resources to prevent and mitigate digital harms and risks.

Furthermore, as outlined in the communal coping model [143], coping with challenges is a "social process" that draws in others (e.g., parents, peers, schools, mental health professionals) who confront the problem individually and together. Instead of individuals independently managing their own stress or challenges, communal coping involves a shared perception of the issue, collective action, and shared responsibility. Like other coping strategies, communal coping is not a straightforward, calculated, two-phase procedure of evaluation and action. Instead, its course tends to be more complex, involving a series of iterative assessment-action cycles [143]. We view our research through a communal coping lens by examining help-seeking in response to digital threats through a multi-stakeholder approach.

This process may incorporate both conscious and unconscious actions, with the communication of these actions potentially not being communicated verbally. Some of these actions could be beneficial, harmful, or have no significant effect on the individuals involved and impact their situation [143]. The display of communal coping is often not so much a product of a calculated decision, but rather of certain facilitating conditions being met [143]. Both social ecological support and communal coping perspectives foreground the embeddedness of help-seeking into a social context, and the importance of relationships and circumstances to whether and how others are involved in communal coping.

Therefore, it is important to untangle the social and contextual dynamics of support by examining the interplay and salience of different support resources

and their relationship to different types of risks, as well as facilitators and hurdles, and benefits and costs of communal coping in response to digital harms and risks because it helps us to see a studied phenomenon in a new light. Examining these issues through the lens of ecological theory and communal coping can provide a holistic and interconnected perspective on the dynamics of help-seeking behavior in the context of youth digital abuse. Addressing digital abuse requires a nuanced understanding of both the opportunities and barriers to help-seeking inherent in digital environments. Our study expands boundaries of ecological and communal coping theories to accommodate digital abuse situations, and offers new perspectives regarding the needs of individuals in digital abuse situations.

4.3 Methodology

To obtain a comprehensive understanding of help-seeking behavior, we analyzed youths' help-seeking behaviors when encountering digital threats and harms using a dataset previously collected from interviews with 101 participants focusing on more general threats and harms, as reported in Chapter 2, Section 2.3. We reanalyzed the dataset using perspectives of both youth and adult stakeholders to address the questions about youth's help-seeking behaviors and the challenges they encounter in reaching out to and using various support resources.

4.3.1 Limitations

This research has several limitations. This study focused on U.S. residents, which included youth from 5 states and adults from 13 states. This might limit the scope

of experiences across different cultures, countries, and educational systems. We also acknowledge that access to support services and resources may vary based on country and state. There are also standard limitations tied to self-reported data that include recall and observer bias.

Additionally, although we included a broad group of participants we recognize that they might not fully represent all experiences, backgrounds, or support systems that can impact young people's digital safety. Key perspectives such as non-parental caregivers and police officers were not included in this study. We also did not actively recruit individuals identified as attackers while focusing on youth help-seeking experiences. However, our findings identified that youth could be victims in some contexts and aggressors in others. Finally, this study did not aim to compare experiences across different groups of youth. The design was to capture a broad range of experiences with help-seeking resources and services. Most of our participants are female, which could create gaps in our findings since digital abuse affects all genders.

4.4 Multiple Pathways to Help-seeking

We frame the help-seeking experiences shared by youth and the stakeholders that support them in four parts: (1) obstacles and deterrents to youth's help-seeking; (2) help-seeking pathways; (3) challenges with help-seeking pathways; and (4) the importance of reliable support systems.

A note for readers. Some quotes, accounts and findings refer to physical or sexual violence among youth and may be disturbing.

4.4.1 Obstacles and deterrents to youth help-seeking

Youth, parents, educators and advocates described the sociotechnical complexities that discouraged or prevented youth from getting help in the face of digital risks and threats. This took the form of desensitization of youth to violence, pressures to adhere to societal norms, cultural expectations, and fears of negative reactions that discourage help-seeking. Additionally, obstacles related to access, awareness, and trust in the digital realm impeded their ability to seek help.

Self-reliance before seeking external help. Our data highlighted the complex nature of interactions within digital spaces, especially in the context of escalating threats such as extortion and sextortion. A predominant self-reliant ethos emerged, shared with us by youth who experienced these attacks. Youth tended to delay asking for assistance when they first encountered digital threats or abuse and shared with us that they did not seek external help and tried to resolve matters themselves.

> "*One time there was this kid and he told me he lived nearby and he came off as super cool and then he started getting creepy and he was overly aggressive. Then I found out he was some older guy and he was catfishing girls. And once I found out about it, I yelled at him pretty bad and blocked him, you know, good for me. Some people just come off as just straight creepy, like random people that add me on Snap and be like, oh, like send pics and I'd be like F-you bye. Like, no, what is wrong with you? They'll add you and just straight send you pics of themselves and then you have to block them because they're weird.*" – Youth, Y95

Navigating the complexities of digital abuse among youth, we uncover sev-

eral reasons that may deter them from seeking external help initially, prompting their preference for self-reliance. An overwhelming theme that emerged is related to the sense of agency and self-efficacy among youth. As they navigate their identities, they foster a culture of self-reliance, often preferring to handle digital abuse independently, even when they encounter fake social media accounts from which perpetrators tried to intimidate and extort, as illustrated above. A desire for trying to handle things on their own may be reflective of societal norms (e.g., what a particular social group or culture considers acceptable behavior) or simply a perceived lack of access to external support they are comfortable connecting to. Additionally, adolescence (ages 12-18) is a time developmentally when youth are exploring their identity, testing boundaries, and establishing autonomy [71, 72, 110]. This underscores the importance for support structures that align with youths' desire for autonomy and need for safety.

> "*"When it comes to dealing with stuff like online nastiness, us kids often handle it on our own. It's like the teachers don't really get all the stuff that happens online. I wouldn't care for teachers to know about this or fighting because it's none of their business and we can take care of it."*" – Youth, Y97

Youth avoid help-seeking due to desensitization.. Another deterrent for initiating help-seeking is a significant degree of desensitization to violence among youth, likely because of frequent exposure to explicit and violent content within the digital spaces that they navigate. Several teenagers expressed to us that they forwarded videos even if they included non-consensual intimate imagery because they were already being shared. Some youth described being influenced by their peers. They told us they saw nothing wrong with "leaking it," a term some youth used to describe forwarding an image. This reflects a social normalization

in the youth culture of the creation and sharing of explicit and intimate imagery as commonplace and unproblematic.

Such desensitization may impair a youth's ability to recognize digital abuse as an issue needing attention, highlighting a concerning issue that demands proactive steps. A youth shared with us,

> "*Yeah, some guy actually texted me, asking me for him to be my sugar daddy or something and I blocked him and he looked super, super old. . . I just deleted it cuz it actually happens pretty often.*" – Youth, Y71

Many youth and adult stakeholders told us that they shared images and personal information without much contemplation or awareness of harm to the person involved, often a person they did not personally know.

> "*I want to add that I think that social media allows the youth to have a false sense of being adults, and so not just this kid because I have other youth that participate in sharing inappropriate photos on social media. But I would like to say I liken it to these young kids feeling a need or desire to be sexual, and this is the only way that they know how to based on the boundaries that are placed upon them from the foster parents. So to answer your question, I don't think that they actively participate and would normally participate in pornography. I think that what happens is, in the heat of the moment, they're sharing, and when the relationship falls apart, it's a defense mechanism. It's a way of trying ... because I'm hurt, now I want to hurt you. So my way of hurting you is by exposing to the world that I've seen you with nothing on or something along those lines.*" – Social Worker, P7

Once these images become public, youth struggle with how to seek help and to navigate these situations. Barriers to help-seeking with sexting and inappropriate photos are rooted in the youth's sense of self-blame for having voluntarily created and shared intimate imagery in the first place, compounded by digital youth culture normalizing such behavior.

This persistent exposure to harmful content and interactions has desensitized youth to such incidents, as a youth noted (Y78), "It's normal to us," illustrating the profound impact of these experiences on her perception of what constitutes an 'ordinary' online experience. The incidents highlight larger societal issues, such as the pervasive nature of explicit and violent content online, and the susceptibility of younger users to such content. Existing support mechanisms accessed by participants, including school guidance and social services, do not appear to effectively counteract the issue of youth becoming desensitized to problematic content. A participant identified the ineffectiveness of school-based internet safety education to adequately address the problem :

> "*When you first get on social media, they give you that little pep talk about cyberbullying and internet safety. And then that was like the last of it until someone in your school happens to get exposed.*"" – Youth, Y78

Youth are skeptical of adults' tech knowledge. Another obstacle to help-seeking is the universally shared skepticism among youth participants regarding adults' ability to effectively understand and handle digital abuse. Even when a parent was seen as a trusted figure, their perceived inability to comprehend the intricacies of digital platforms and situations often served as a deterrent to the youth seeking help from them. This lack of confidence in adults' understanding of the

digital applications (apps) and situations encountered further discouraged youth from seeking support.

> "*I mean, you could report it [digital threats], but it's not really gonna do much, like when your account gets reported on social media, somebody has to report it. They [social media platforms] have to find something like super wrong for them to actually take it down. So it's like the only thing you really can do is block them. And I mean, like I could tell my mom or something about it, but there is not really anything she can do about it because you can't really tell who the person actually is from behind the screen to try to give them an actual consequence. And I mean, she could go and try to talk to them, but they can just like, not answer you know?*" – Youth, Y79

This highlights inadequacies in the current system for protecting youth from nuanced forms of online harassment. Additionally, the anonymity of the digital encounter is a barrier to holding the perpetrator accountable. Even when adults are available to intervene, the lack of options, choices, and consequences to identify the perpetrator are recognized by youth as limitations and deterrents to help-seeking. These findings draw attention to the need for more effective measures and options for mitigating digital threats for youth.

A similar sense of inadequacy for mitigating harms caused by digital abuse was expressed among youth receiving support services. Because these support services were designed to address issues outside of digital abuse, such as family situations related to domestic and or sexual violence, youth did not view these advocates as resources to assist with digital abuse mitigation.

> "*I didn't know I could talk about the app stuff here, my social worker doesn't*

even know the apps I'm on. If they asked us about it or held some kind of a group I guess we'd discuss it." – Youth, Y88

Despite having support systems in place, some youth did not share digital threats or abuses. Youth participants receiving services communicated that technology safety was not something discussed so they did not share their digital abuse experiences in individual or group support programs.

Negating the concerns of youth seeking help can silence them. Despite adhering to the advice of reporting instances of cyberbullying or online harassment to educators, youth disclosed that their complaints were disregarded or downplayed. Both youth and parents often shared incidents in which conflicts unfolded in the digital world, only for the school principal or director to request screen- shots of the altercation and then attempt to interpret the situation out of context (through screenshots), ultimately undermining its seriousness and the respective consequences.

"*I got cyberbullied. My parents say tell the teacher, tell the school, and that is what I would always do. But the person who bullied me, she had a way of lying and the school did nothing. They asked for screenshots of my personal conversations. They would always still put us in the same classes. They'd make us work together and stuff like that. After that stuff happened, I was just really quiet. I just took it. It sucked.*" – Youth, Y84

This illuminates the complexities of addressing cyberbullying within an educational setting and emphasizes the importance of appropriate responses from authorities. It underscores that ignoring or inadequately addressing such

com- plaints can lead to feelings of hopelessness, further victimization, and silence among those youth impacted, including their resistance to reporting future incidents. Additionally, when schools request excerpts of digital exchanges by which to determine severity, the lack of technical understanding or awareness of manipulation of content (e.g., deepfakes) can lead to perpetuating the cycle of abuse.

Fear of negative consequences. Youth participants shared their concerns that parents or other authority figures may not fully comprehend the problem or may overreact by implementing restrictive measures, such as taking away their digital devices, prohibiting contact with certain friends or limiting access to social media. Many youth told us that this fear drives them to postpone or avoid consulting parents or other authority figures. As one youth participant shared,

> "*I want to handle things privately without the whole world weighing in, unless it is something that goes too far.*" – Youth, Y66

This intricate balance highlights the need for more anonymous reporting both in the digital and physical worlds in order to provide secure and private reporting channels. Ultimately many youth preferred, across all digital threats and abuses encountered, to prioritize their privacy and their ability to resolve the situation independently, often not recognizing the severity of the digital threats and impact on their safety.

Self-blame coupled with anxiety impeded help seeking. Additionally, if they felt they did something wrong to cause the digital abuse, such as sending an image or engaging on an adult platform, this feeling of responsibility and self-

blame created additional concerns and fear about getting in trouble for initiating the digital interaction that led to the abuse.

> "*I remember feeling like it was all my fault, you know? I was the one who decided to send that picture. I felt anxious from that, or what consequences I might face...it just made me feel like I couldn't tell anyone. Like, how could I? I was the one who did something wrong in the first place. It was scary and lonely. Finally my parents found out from a friend of mine's parents and they (my parents) took my phone.*" – Youth, Y83

Lastly, in school settings, one primary obstacle to help-seeking among many youth was the fear of blow-back from one's peers and perpetrator if they were to report abuses perpetrated by another student. Often youth struggled with guilt, anxiety, social stigma, betrayal, and the fear of retribution that could follow. We identified a prevailing uncertainty centered around snitching that often hindered the reporting process.

> "*just feel like the whole topic of snitching and actually telling somebody when there is an actual problem, I just feel like it is really hard to distinguish when you are snitching and when you are not. The thing about snitching is that there is a stigma around it. If you snitch, you are snitching against the kids basically. It is a bad thing to snitch.*" – Youth, Y96

After identifying obstacles and deterrents we now describe the help-seeking pathways described by participants.

4.4.2 Help-seeking pathways

Many youth and adult participants described why youth sought or avoided help when confronted with digital threats, leading to the emergence of two distinct pathways: youth-initiated and pathways initiated by others.

Youth initiated pathways

Youth shared with us that their decisions to seek help in response to digital threats are influenced by a complex interplay of factors, including their support network, socioeconomics, fear of negative reactions, prior exposure to digital abuse, and proximity to the abuser. The willingness of youth to seek help was intrinsically tied to their perception of potential consequences, good or bad, arising from disclosing digital abuse.

Youth seek help when things spiral out of control. Fear of a situation escalating or recurring prompts youth to seek help. Youth and advocates shared that they may seek help by confiding in a single individual and sharing specific details about the issue they are facing when "things spiraled out of control." In these scenarios, they may want others to get help for them when they feel they are unable to do so. This approach involves entrusting "a little bit of information to just one person." It is important to recognize that the act of seeking help goes beyond the mere decision to do so and includes many pathways and strategies employed by youth as they reach out for assistance, highlighting the intricacies and nuances of their help-seeking behavior. An advocate shared,

"*So, they can be scared online. Something will happen online where the*

perpetrator will say to the youth, "Send me more pictures now or I'm going to send the pictures that I have to your family members." That could be some sort of threat, and that's sextortion. So when it gets to that point is really when I see it as a breaking point, when there's actual threats to others and the teenager is realizing, 'Oh no, this person is not being the loving, caring, nice person they once used to be' Oftentimes, these teenagers, they will disclose a little bit of information to just to one person, and just enough information for them to be concerned about what's going on and if they are a mandated reporter than it gets referred. Most of the time, I will get referrals from other social service agencies and schools."" – Advocate, P32

Participants shared with us that there are instances in which fear of escalation prompted them to tell a teacher at school rather than their parents, often due to an underlying fear of losing "digital privileges" (access to technology). These instances included youth encounters with strangers they met online who were revealed to be perpetrators. This fear of "getting in trouble", demonstrates a key predicament that many young people grapple with, calibrating their disclosure choices or deterring them from seeking adult intervention all together even in situations that have escalated online to the extent that the youth feels unsafe.

"*The student approached me during class and we stepped out in the hallway. She was telling me about how she was on Facebook. This person had friended her and a bunch of other people in her community. He contacted her to video chat and then flashed her and she didn't know what to do about it. She worried that if she told her parents, they would take away her phone. In that instance, I reached out to the principal and I said, you know, this is really serious. I should have made a mandate. I should have made a report then.*"

– Educator, P46

This highlights the role educators can play in providing support and intervention. In this situation, the student felt comfortable enough to confide in a teacher, suggesting that schools can serve as an alternative or supplemental support pathway for youth dealing with digital threats. Furthermore, youth fears were compounded in situations where the potential ramifications of reporting extended beyond loss of privileges to concerns about family welfare. Youth from vulnerable backgrounds such as families worried about immigration status may not reach out at school and refrain from reporting due to anxiety about attracting unwanted attention from Child Protective Services.

Youth balance and negotiate the anticipated costs and benefits. This factors not only into their decision of whether to seek help or not but also to whom to confide. The teacher's immediate action to alert school administration emphasizes the importance of having a clear and effective response protocol within educational institutions to address instances of digital harm.

> "*I've seen situations where kids just don't do anything about it and have to deal with it. I guess a lot of people might go to their parents depending on how they feel their parents will react. Some people just go to the school about it and they swill obviously bring in the police because it's child pornography and it's illegal and they'll try to find the person that exposed them and you can get charges pressed. They'll try to track down the few people that have it and ask who did you send it to? And try to make them delete it. It's not like the police can really do anything about it to make it stop because once one person sends it and then everybody has it.*" – Youth, Y81

Youth balance and negotiate the anticipated costs and benefits. This factors not only into their decision of whether to seek help or not but also to whom to confide. Some participants expressed approaching reporting via a threshold of harm that determined whether or not they would seek-help and disclose the threat or attack. In these instances participants described weighing the potential harm of disclosure and how it would impact them personally versus their possible moral obligation to report harm directed at someone else.

> "*If I see something really bad going on then I am going to go say something. If it is something where someone is going to get hurt then obviously I am going to go tell someone.*" – Youth, Y99

Youth frequently find themselves at a crossroads when they encounter digital threats, attempting to strike a balance between self-protection, the desire to defend themselves, and their concern over the possible fallout from seeking outside assistance.

Help-seeking initiated by others

Youth receive help after others initiate disclosure. Several participants shared that accidental disclosure led to the initiation of help-seeking behaviors. In these situations the disclosure stemmed from external sources. Siblings or neighbors unknowingly found themselves igniting a chain of help-seeking by sharing seemingly inconsequential details in casual conversations.

> "*A lot of the time parents find out through accidental disclosure, it didn't come exactly from the child. I have cases in which the younger sibling was*

in the house when the older sibling started inviting people over. So it came up in a random conversation with a child saying, "Hey so and so's friend came over the other day again." And so the parents like, "What friend?" That's how that came out. In other cases, it has been because neighbors have told the parents that they have seen suspicious activities. It's because the children are behaving so badly that the parents try to take away cell phones. And once the parents go through the cell phones they realize that they have had these really inappropriate conversations with some random stranger."
– Advocate, P48

In this context, 'help' is summoned not directly by the individual navigating the threat, but indirectly by the collective community [143] concerned about youth well-being. In these scenarios, adults may find themselves thrust into the role of help-seekers through discovering their child is engaged in vulnerable situations online that require intervention. This reveals that youth may lack digital literacy skills and/or the ability to navigate potential threats independently. The need for others to step into the role of help-seeker underscores the importance of family and communities in the digital safety of youth. However, this also raises issues of trying to provide protections for youth privacy, trust, and safety. Accidental disclosure highlights the nuanced aspect of help-seeking that draws upon a community to enact safety protections beyond the individual user and the interrelated aspects of the digital and physical world.

The common pathways that youth interfaced with. The various stages in a youth's journey with digital abuses are not linear or homogenous. There is no one single stage in a youth's journey with digital abuses that they can be said to "seek help." Youth may engage in help-seeking after repeated attacks, a

single attack, or when the frequency or quality of attacks reaches an untenable threshold. We cannot point to any one trigger that drives youth to immediately seek external help. As noted by one of our youth participants,

> "*Somebody would contact me like 20 times during the night. Then I kind of blocked them and then deleted them. But it happened to me more than five times on social media. . . I would get messages asking for pictures, in return for money. And obviously like I am young, so I was freaked out, you know? I didn't know how to handle the situation.*" – Youth, Y80

Multiple entry points

There is no single help-seeking journey. Our data reveals the recurrent nature of digital abuse many youths endure before initiating help-seeking processes. The key factor to understand is that there is no one-size-fits-all approach to help-seeking, as it can be influenced by numerous factors including living conditions, socioeconomics, peer network, community support, digital literacy, age, and even desensitization to abuse. All these variables may contribute to which of the various sources of support are used. We can think of these in terms of help-seeking entry points into a help-seeking system that youth might be more likely to engage with.

Youth may initiate help-seeking themselves or through the support of friends, family, educators, or mental health professionals. Our data has identified a number of pathways taken by youth to enter into help-seeking journeys. The distinction being made here is not the help-seeking itself, but the possible entryways or catalysts for the help-seeking and help-resource portion of a youth's

journey to commence.

In Table 3 "Entry Point to Help-Seeking Pathway", we explore various entry points or catalysts that prompt the help-seeking journey of a young person dealing with digital abuse. This table is based on an analysis of our data which identified these pathways across the digital threats and harms youth experienced. These pathways can be initiated either by the youth themselves or by other individuals or institutions. For example, the *"Self-Disclosure"* pathway is initiated by the youth when they recognize their own situation as digital abuse and proactively seek help. This proactive initiative is also seen in the *"Self-Education / Information Seeking"* pathway where a young person becomes aware of their experiences as abusive and seeks information on digital abuse. Other pathways like *"Peer Recognition"* an *"Guardian/Adult Intervention"* can be initiated both by the youth or by peers and adults who notice changes in behavior or signs of distress. This dual-direction initiation is also seen in pathways such as *"Tech Companies," "Mental Health Intervention,"* and *"Legal Intervention."* Some pathways like *"School Intervention"* and *"Involuntary Disclosure"* are typically initiated by others, not the youth. In these cases, school officials or other adults become aware of potential abuse situations and take action. The *"Community Outreach"* pathway offers an anonymous avenue for help-seeking where the youth can reach out to community resources like support hotlines or apps. The *"Post-abuse Investigation"* pathway generally comes into play in severe cases of digital abuse leading to serious harm.

Recognizing and understanding these pathways and their influencing factors allows for a more nuanced and comprehensive view of how youth navigate the challenges they encounter in the digital help-seeking ecosystem. It helps us

identify where interventions can be most effective, and provides an opportunity to develop resources that are flexible, adaptive, and responsive to the individual needs of youth. This holistic perspective can yield more effective strategies, aiding youth through their cyclical journey to recovery from digital abuse, and ensuring support mechanisms are in place for their continued resilience in digital environments, recognizing that abuse may perpetuate and cross over from the digital to physical world.

Entry Point to Help-Seeking Pathway	Description	Pathway Initiated by Youth	Pathway Initiated by Others
Self-Disclosure	The individual recognizes their own situation as digital abuse and proactively seeks help.	✓	
Peer Recognition	Peer groups notice changes in behavior and intervene or encourage intervention.	✓	✓
Guardian/adult Intervention	Parents or guardians detect signs of distress in the child and/or observe something on the child's phone and take action.	✓	✓
School Intervention	School officials recognize potential abuse situations through reports, harm, and software.		✓
Tech Companies	Awareness of abuse through user reports or detection systems. Removal of abusive content.	✓	✓
Mental Health Intervention	Mental health professionals detect signs of digital or physical abuse during therapy or counseling.	✓	✓
Community Outreach	Youth seek help anonymously by reaching out to the community (support hotlines, apps, etc.)	✓	
Legal Intervention	Legal authorities intervene upon becoming aware of abuse during criminal investigations or from direct reports of abuse.	✓	✓
Involuntary Disclosure	Unintentional discovery of digital abuse.		✓
Self-Education / Information Seeking	Youth recognizes experiences as abusive and seek help by searching for information on digital abuse.	✓	
Post-abuse Investigation (severe cases)	After digital abuse leads to serious harm, authorities or digital platforms investigate, or parents initiate an investigation.	✓	✓

Table 3: Entry Point to Help-Seeking Pathway

To reiterate, there is no single point or threshold at which a youth consistently begins and ends their help-seeking journey. Our research has identified a set of 11 help-seeking starting points or entryways iterated in Table 3. These help-seeking entry points can be broadly grouped into two classes - voluntary and self-initiated or involuntary and externally initiated. Next, we'll analyze common challenges experienced by youth in their help-seeking journeys.

4.4.3 Challenges with help-seeking pathways

Youth entanglements in formal support systems. Situations of digital abuse occurring within school environments (cyberbullying and harassment) sometimes inadvertently reached the awareness of educators, as these issues moved from the digital world into physical interactions or vice versa. In these instances both the youth perpetrating the abuse and the youth victim become entangled in formal support systems that, in the process of trying to mitigate harm and prevent further threats, can wind up causing additional concerns such as retaliation or involvement of social services or law enforcement. Moreover, the school's response can be punitive and youth and parents described being subjected to embarrassment, reputation damage, and further digital threats due to getting a peer in trouble. A parent shared with us:

> "*An incident happened at school with my child in middle school where they were accused of hacking or stealing a Facebook account from a girl. The school did not share with me or ever show me what happened. I didn't know to ask. They were accused of posting a nude baby photo on the girl's Facebook. He was very scared and intimidated because the school called the police and*

they came with handcuffs in their hands. It was a scare tactic. They were told that if something like that were to happen again, the police would come back and would arrest him next time. Oh, they also punish him by saying that for four months they had to hand write repeatedly on the blackboard about sexual harassment and sexual assault."" – Parent, P5

Police involvement and intimidation tactics were familiar to advocates providing support to vulnerable youth. They described how fear and punitive measures could be detrimental by discouraging youth from seeking help in the future. The punitive environment shared with us by many stakeholders underscored systemic issues in managing digital misconduct in educational settings. The need for enhanced communication, proportional disciplinary measures, and an open, supportive environment was echoed by many stakeholders.

These insights reveal several important issues related to the process of seeking help in instances of allegations of digital misconduct with a minor, in this case a middle schooler. Many parents identified that there was a lack of clear and comprehensive communication with educational institutions regarding incidents in which youth were accused of digital abuse. Parents shared that they had a lack of understanding as to how to navigate the communications with schools regarding digital threats and therefore felt they could not effectively intervene or provide guidance. Several parents explained if a fight breaks out at school people see it and as a parent you get a sense of what happened. But when there are accusations regarding digital threats "you can't go through all the other kids phones". This further highlights the need for policy that is designed specifically as a means of protection for both the youth victim and potential youth instigator during these formative years of development.

Lack of a shared terminology. Educators shared ways that they tried to engage students in cyberbullying education when formal programs were lacking within their schools. Through a vocabulary exercise around this concept, one educator explained how they uncovered a youth's exposure to catfishing. The youth shared that despite being subjected to constant attempts to gather personal information by a stranger, they did not seek help or advice, indicating a lack of understanding about the threat she encountered. An educator shared with us,

> "*"I did an assignment with my fourth grade students where I gave them vocabulary to write sentences about their understanding of cyberbullying. A few vocabulary words into the assignment a fourth grade student described getting catfished on Roblox she said, 'They were asking her date of birth? Where did they live or go to school?" She said that she didn't end up telling them where she went to school because she got leery about it. It was a couple days' worth of them asking, and they would always be on when she was on and ask "So, when you coming on to play again?" And she would tell them. I had to explain to the students it's more than just catfishing it is dangerous. And she laughed about it. I'm like, That's not really laughable.*" – Educator, P4

Many stakeholders (educators, parents, and healthcare professionals) struggled with understanding the vulnerabilities inherent within digital platforms and the terminology youth used to describe their experiences. For example, terms like *cyberflashing, airdrop, and deepfakes* were readily understood by youth; however, many stakeholders throughout the study often asked for explanations or clarifications regarding the meaning of the term and how technology could be used to enact harm.

Stakeholders shared that they needed education and training to be aware of the digital landscape and potential threats these youth might encounter, such as cyberbullying, online sexual exploitation, or recruitment by perpetrators. Our findings highlight the importance of also educating youth about internet safety and help-seeking, with a particular focus on using a shared terminology allowing for recognition of digital signals of distress as well as how these might impact youth in the physical world.

Additionally, adopting shared terminology creates an inclusive environment that encourages youth to seek help and discuss their experiences without the burden of stigma. A shared vocabulary can reduce stigma, and empower individuals to openly discuss digital risks and attacks, seek support, and engage in conversation. We now discuss the help-seeking pathways that youth engage with when faced with digital threats and attacks.

Stakeholders have competing interests that lead to inefficiencies with receiving help. While different adult stakeholders work toward the same common goal of supporting youth, in reality, their interests may diverge and even compete with one another. Advocates shared the challenges of dealing with cases where a parent, law-enforcement, and the youth survivor are all voicing different preferences. Parents often exhibit willingness to cooperate with ongoing investigations regarding potential abuse or illicit activities involving their children. This includes providing information, allowing access to their homes, and engaging in interviews, demonstrating an active stance in seeking help from authorities to address possible problematic behaviors in their children. However, barriers to this process often manifest around the issue of accessing the child's mobile phone. Some parents harbor fears about the potential confrontation with their

children, leading them to resist turning over their phones to authorities. This reluctance hinders the investigative process, withholding critical evidence.

> "*We've had parents who are afraid of confrontation with their children over their phone. So they just decide not to comply with that. They are willing to comply with the entire investigation about whatever their children's abuse is, but when it comes to the phone, they don't want to get in trouble. So they just don't want to give it up to the police.*"" – Advocate, P52

Further complicating matters are the cases where parents have knowledge of their children's illegal activities beyond the initial scope of the investigation, such as drug-related texts and meetings. These parents feel partially responsible or fear further legal complications, thereby forming another barrier to the acquisition of the child's phone.

> "*Then unfortunately you also have the parents who know that their children are doing something more than what the abuse is like, you know, texting about illegal substances and stuff like that. And meeting up with people to share drugs and stuff like that. And so the parents somehow feel like it's their fault. they don't want their children to get into more trouble. So then they just don't wanna give up the phone. And then you also have the parents who are either pushing their own children. And so that's why they're afraid of the phone being given up.*"" – Advocate, P53

Difficulties in accessing youth devices create obstacles for child protection. Another obstacle arises when parents are themselves implicated in the abuse of the child. Advocates shared with us that in these situations, parents are afraid

of self-incrimination and therefore are hesitant to give their child's phone to investigators. This process can be further complicated by varying local and state laws. In some states law enforcement procedures necessitate explicit adult consent before they can access a child's phone.

> "*One of the things that our detectives keep bringing up, is changing the law for the state regarding consent. if you wanted to get possession of devices belonging to a minor but the parent won't give it to you - you'd need a search and seizure warrant. Meaning not only do you want to search it, but I want to take it without the subject's permission. So you'd have to put in the affidavit — the parents are the suspects , here's why we have reasonable cause to believe they are responsible and it will have evidence that can be easily erased etc — and then a judge would have to grant it.*"" – Lawyer, P44

The complications arising from parental involvement in abuse and the intricacies of legal procedures underscore the multifaceted nature of the digital threats and attacks that entangle youth into help-seeking systems in which policy, privacy, trust, and safety collide. We now explore the challenges that arose between parent and child in efforts to establish digital safety.

Parents' challenges because of a lack of knowledge and understanding. Another help-seeking predicament is related to a lack of knowledge and understanding around online safety and digital threats. Some parents implemented protective practices, which included guidance on not talking to strangers, but did not think to follow through by checking with their children about worrisome incidents online. Several youth participants implemented this advice but never

told their parents that they had a risky encounter in which a stranger approached them online.

> "*So, my mom says, be careful, on that type of game, because you can chat with people on there and she told me some people are on there to basically online date. So, my mom says not to do that, because there could be people that could be old people and they're trying to get with kids. I see a lot of people doing that on Roblox, but I just don't talk to them because they clearly don't know the safety of that and stuff. Usually when I'm in Roblox and someone is making me feel uncomfortable, I just instantly leave the game and block them.*" – Youth, Y89

Notably, participants aged 10-11 did not know to tell adults about digital threats they encountered. Youth clarified that they were not trying to hide this from their parents or guardians but, "just did not tell them" as they were not asked by anyone. Youth chose not to disclose these encounters to an adult because they were self-engaged in preventive practices or did not feel it was necessary or didn't think to do it. Our data surfaced the importance of including both digital safety with youth by asking them about their online experiences, any potential concerns or experiences they have had online, as well as including safety practices.

> "*Sometimes when I'm gaming, a random person talks to me. I just leave, and I lock my door to my house because I don't trust that person.*"" – Youth, Y85

The actions these children undertook, such as hiding or securing doors, hinted

at their fear but simultaneously indicated the child's lack of understanding of the threat's severity.

Many parents communicated challenges in managing their children's safety and, in turn, their technology. They expressed a need to control their child's access to specific applications, indicating a concern for their child's online safety and exposure. However, their self-admitted lack of technology knowledge posed a significant barrier. Challenges in finding resources or places to facilitate learning and a lack of understanding of technology prevented them from implementing the digital safeguards they wanted to enact to protect their children.

> *"No, I have no resources. I've looked at a few apps, like in the App Store, to see... There were a few apps that say something like limit how many... I guess put limitations on other phones in the plan. I am not technology-savvy. I think I just got a feel for how to operate an iPhone. And I know my limitations. I don't have the technology base inside of me. I do have family members who do. I just feel like, for them, for me to ask for that is like... I don't know. It's like they feel like it's so tedious. Like, "I can do it for you, but it's tedious." And, I don't know. People don't really want to make time for that. And I don't want to impose any burden, or any more responsibility than they already have. So, no, when it comes to resources like, I'm at a loss. I would love it if there was an app where I could just press a button and remove whatever I want from their (child's phone for the moment.) Like, "Nope, you can't use Instagram, TikTok, Twitter, until tomorrow morning." I would love an app like that. I would love something that I can control through my own phone, so that I don't have to take their phone and fight for them. I don't know much screen time and if there is anything to work with*

there."" – Parent, P30

Help-seeking limitations. Youth and adult participants expressed feelings of frustration, helplessness, and confusion when trying to figure out how to address attacks. Digital abuse involving non-consensual intimate images often presented the greatest challenges. Participants described considerable limitations in the existing help-seeking pathways, which they described as inadequate to effectively help youth victims mitigate the repercussions of these attacks. Youth shared with us that it is difficult to get content removed even if it was reported on a social media platform.

> "*I've seen situations where it's just like, kids can't do anything. Like they just don't do anything about it and they just have to deal with it. . . Once you're exposed (non-consensual intimate images), it's like, you can try to get back at the person, l press charges, tell them to stop sending it. But it's not really a way that you could ever really fully stop it.*"" – Youth, Y91

Despite youth recognizing that options exist, including legal intervention, personal requests to the attacker, and reporting to the platform, youth participants felt a sense of powerlessness communicating that they believed they were unable to halt the continued dissemination of these non-consensual intimate images across social circles.

4.4.4 The Importance of Reliable Support Systems.

Participants shared with us divergent experiences of who they thought was responsible for keeping youth safe online, including formal and informal help-

seeking pathways. Youth also expressed a lack of knowledge with help-seeking, which was a recurring theme. Many youth were unsure about how to initiate the process when they encountered digital threats and attacks, indicating a significant gap in current educational and institutional structures. Many youth and adult participants expressed their expectations of how digital safety for youth could be expanded. They also shared the most challenging situations to resolve, both online due to the proliferation of content online and offline due to repeated cycles of abuse from either the perpetrator or others. These findings provide insights into their lived experiences and expectations, serving as a foundational guide for the continued expansion of digital safety measures that align with youth help-seeking need

Proactive advocates engage at-risk youth. When advocates engage at-risk youth, they shared with us their process of supporting youth in the challenges that youth experienced, coping with harms both in the digital and physical world. Building trust and looking for patterns of behavior and signals helped them identify potential threats youth might be up against based on their experience.

> ""*As professionals reaching out to vulnerable youth, I understand that every community has at-risk populations. These youth are more prone to trafficking, exploitation, or being targeted by predators, either in-person or online. In my own community, which is quite rural and has a large Native American reservation, I identify a significant portion of our at-risk youth. The risks often present as gang involvement or transient living, such as couch-hopping. This type of homelessness, where youth move from couch to couch, is a significant red flag. Other vulnerable groups include LGBTQ or two-spirited youths, and those involved in the foster care system. I look*

for the signs and this helps me think of what could be happening in their virtual life. This approach helps me to be alert to potential issues they might be encountering in their online life as well."" – Social Worker, P9

Expectations of safety features. Many youth wanted to know more about safety and felt that apps should provide more information about how to "identify a shady account," along with information about ways their safety could be compromised by features they are using. They wanted resources made available by the platform that aligned with the threats they experienced. Some youth participants expressed that other youth may not have a clear understanding about what an app provides in terms of security and privacy settings. Concerns about location sharing on platforms that included shared location features such as snap maps noting they sometimes forget it is on. Young individuals also warned that teenagers might overestimate the efficacy of in-app reporting methods while also expressing worry about interconnected threats across various platforms.

"*I think teens should know more about the safety features that the apps have, because, like they're (teenagers) and are just gonna assume the app has a safety feature where they could report this person and the app is gonna do something about it. I would like somebody to teach me how to get more resources because it could lead to other things. The companies and apps should let us know that somebody contacting you on Instagram is also contacting you on another platform , or that maybe you forgot, you had your locations on, on snap and some predator finds you on snap. The apps should let people know what these apps are really doing?*"" – Youth, Y84

Preventing unwanted interactions. Youth engaged in help-seeking behavior by

using security features on digital platforms to block or mute individuals who posed a threat to their safety. The ability to control their digital interactions through these features was a crucial part of their self-protection toolkit. Several youth explained how they manage and mitigate experiences of online threats, as well as to proactively prevent unwanted interactions. This use of blocking and muting features was part of a broader digital help-seeking behavior framework, which included not just direct requests for assistance (reporting to the platform), but also indirect actions taken by youth to mitigate threats and/or try to resolve issues.

Navigating challenges of blocking and reporting features. While youth appreciated the existing measures like blocking and muting as immediate defenses, they were aware of the limitations. They pointed out that individuals they blocked or reported for inappropriate behavior can sometimes reappear with a new account. Youth saw this as an opportunity for platforms to strengthen their user monitoring systems across platforms.

> "*On social media, you can report somebody. That person could be off of that app and then just get to you on another app. Yeah, I got reported for something I said to somebody. I know people got their account reported, and they made a new account just to connect back with somebody. They need to have a way that you can just block people on all accounts at once.*"" – Youth, Y74

Opportunities for enhanced privacy and anonymous reporting. Youth also identified platform reporting as another area for improvement. They suggested that anonymous or confidential reporting mechanisms could encourage individ-

uals to report digital and physical threats without fear of retaliation or social stigmatization. As one participant shared,

> "*They really gotta do something to protect our privacy, both in school and on social media. Seriously, that needs to change.*"" – Youth, Y93

Linking digital and physical safety. Moreover, youth highlighted the interconnectedness of the digital and physical worlds. They emphasized the importance of understanding this connection, particularly in scenarios where online conflicts could potentially lead to offline altercations. This feedback highlights the complexity of their digital experience and the need for comprehensive safety solutions considering the intersectionality of online and offline environments.

> "*The kids that are fighting, fist fighting gets recorded. It expands everywhere. It will get transferred to different social media and stuff like that. So that's how it goes viral in school, sometimes it starts when kids will say something [have a disagreement] during school and then it moves to social media and then they fight. I remember one time when we had a fight at my school and people from all over State were posting it within the first hour.*" – Y77

The need for trusted resources. Youth participants said that they thought that pointers linking them to trusted resources would be helpful. This highlights the need for platforms to raise awareness about security measures and for the creation of tools to assist users in efficiently managing their expectations of online security and privacy. Additionally, this underscores the necessity of raising youth digital literacy to mitigate potential privacy and security threats.

Adult participants also echoed this sentiment, emphasizing the lack of educational resources regarding digital safety. They shared their perspective, signaling the importance of a holistic approach to online safety, one that not only relies on the user's vigilance but that also involves educational institutions in fostering a digital safety environment.

> "*The big thing is the lack of resources in terms of education internet safety. Because, not a lot of parents know that there are certain things that you can do to prevent your children from using, accessing these types of sites and dangerous Apps. I think addressing the issue before it becomes a problem is something that really needs to happen in terms of the legislature. Having schools brings up Internet safety because it's required of them and that's already a place that parents rely on and deem a safe place for their kids. Internet education should be part of a school wide curriculum or school wide event that parents have to attend or children have to attend.*" – Educator, P12

Youth and adult perspective highlight the need for holistic digital safety education and resources. These findings provide insights into their lived experiences and expectations, serving as a foundational guide for the continued expansion of digital safety measures that align with youth help-seeking needs.

4.5 Discussion

Our findings provide a complex digital help-seeking ecosystem describing help-seeking behaviors of youth in response to digital abuse, the events that precipitate

help-seeking, the support systems that youth engage, as well as factors or obstacles in their immediate environment that influence their willingness to engage with support systems. First, we discuss the challenges and opportunities inherent within the digital help-seeking ecosystem. We also propose a framework for stakeholders and the HCI community to take into consideration when developing tools or programming addressing youth help-seeking in response to digital threats and attacks. Finally, we describe a holistic approach for addressing youth-digital help-seeking behaviors.

4.5.1 Understanding challenges and opportunities to improve youth help-seeking behavior

Our study examined help-seeking behavior of youth in both the physical and digital worlds in response to experiences with digitally mediated threats and abuses, expanding the understanding of the challenges faced by youth and stakeholders when seeking help. Despite the rise in youth exposure to digital abuse, the area of youth help-seeking behavior remains understudied and underdeveloped. Navigating the complexities of digital abuse among youth, we uncovered barriers as well as contextual and relational constructs that deter youth from seeking help. An overwhelming theme that emerges is the importance of agency and self-efficacy among youth in addressing digital risks and harms. These findings align with prior work noting the importance of youth autonomy in managing digital challenges [138]. Additionally, our findings illuminate the need for support systems that align with youths' intrinsic desire for autonomy and with how they identify and communicate their digital abuse experiences. Our

findings highlighted the importance of using terminology that resonates with how youth identify the problems they experience so that there is validation of the youth's experience, as well as policy and protections that align with the threat model.

Addressing gaps in formal support systems. Formal support systems, including those provided by schools and social services, show gaps in addressing the range and complexity of online risks. A significant part of the problem lies in the pervasive exposure to explicit content and harassment on digital platforms, pointing to a critical need for more effective content moderation and safety measures. Our findings expand prior work that shows that youth preferred informal resources to formal resources [180, 153, 232]. However, we build upon this work by showing that youth will use formal resources alone in situations where there is a fear of escalation. Additionally, our research expands upon this prior work by showing the broad range of help-seeking pathways youth use in response to digital threats [180]. We contribute to this body of work, noting that there is no single help-seeking pathway that is uniformly used in response to digital threats.

Additionally, our data show that youth often did not have any digital safety education provided in high school or middle school that aligned with the threats and risks they experienced. Our findings highlighted that the digital world can lack structured support, and the security and privacy features are not clearly mapped to the diverse needs of youth in response to various digital harms and platforms and contexts on which they are encountered.

Challenges in help-seeking and the digital environment. We build upon prior work [191, 28, 133] by showing that the digital divide and inequities in access to

digital resources can further hinder help-seeking behavior for youth as well as the ability for adult stakeholders to provide support. This makes help-seeking in response to digital abuse particularly challenging as it requires not only digital literacy but also an understanding of how to engage with digital platforms to report abuse and seek assistance effectively. In addition, vulnerable youth who do not have access to private, secure internet services may experience challenges in accessing appropriate help. Therefore, addressing digital abuse requires a nuanced understanding of both the opportunities and barriers inherent in digital environments.

Our research also showed that youth often did not perceive adults, specifically parents, as resources as they felt that they would not understand the technology enough to mitigate the digital threats they experienced. Youth described trusted adults as not being "tech savvy" enough to provide support. This perception led to them generalizing this perception and not seeking help at all.

Understanding youth help-seeking across contexts. While youth help-seeking in mental health contexts has been well described, there has been a call to understand youth digital help-seeking in response to a broad range of digital threats and from a multi-stakeholder perspective. Digital abuse often occurs within a sociotechnical system with its own set of norms and expectations.

Our data showed that the process of seeking help for digital abuse is not clear to youth nor the adults that support youth. Stakeholders described that they lacked training to provide digital safety recommendations to families that presented with concerns about digital threats or safety. For example, several stakeholders discussed recommending screen time features or parental control apps but were unable to explain how this could protect youth from specific

threats.

There is a need for an in-depth examination of the help-seeking landscape in response to digital threats to provide perspectives of multiple stakeholders and multiple threats. Our research fills this gap by contributing a qualitative study and describing the perspectives of youth and the multiple stakeholders that provide support, examining help-seeking behavior of youth in response to different threats [78] and across different platforms taking into account how abuse can span the digital and physical worlds concurrently.

Overcoming barriers to youth digital help-seeking. We found a myriad of barriers confronting youth as they sought help in response to digital threats. These challenges to seeking help can include fear, stigma, and a lack of awareness about available resources that align with the threats that youth experience. These were not only experienced by the youth but were also echoed in the narratives of the adult stakeholders, including parents, advocates, and educators. Our findings also emphasize that these challenges did not end with the act of reporting to social media companies or adult stakeholders, but rather continued as youth remained vulnerable to ongoing threats and risks, underscoring a pressing need for continuous support.

In terms of relational influences, the nature of the relationship with the abuser - whether a known peer or an anonymous online presence - can also significantly shape the help-seeking process. Our work expands prior work in showing the support or lack thereof from friends, family, and trusted adults plays a crucial role in enabling or hindering help-seeking behavior [138, 139]. Additionally, the anonymity in digital spaces can facilitate abusive behaviors that are emotionally and psychologically damaging, yet hard to trace and connect to the perpetrator.

Our research also reveals a degree of desensitization to violence, attributed to exposure to violent content within the digital spaces that youth navigate. Such desensitization may blur their recognition of digital abuse as an issue needing attention and demanding proactive steps. When intimate images become public, youth grapple with feelings of self-blame and the task of seeking help becomes even more daunting, especially given the backdrop of a digital youth culture that has unfortunately normalized such behavior. These findings underscore the pressing need to develop youth-centric, context-aware support systems that respect their autonomy, mitigate harm, and foster safe digital spaces.

Our research unveils a troubling desensitization among youth towards online violence, possibly masking their recognition of digital abuse. This issue, coupled with a culture that regrettably normalizes such behaviors, presents significant hurdles for those seeking help. These findings underline an urgent need for youth-centric support systems that are cognizant of this context, promoting safety while preserving their autonomy. As such, it's vital for stakeholders to prioritize the development of strategies mitigating online violence and enhancing digital literacy.

As a result, it is imperative for stakeholders to implement strategies that reduce exposure to online violence and foster digital media literacy among youth [61, 62] and across platforms, including those that support teens through evolving digital encounters. Future work should focus on identifying risk behaviors and continue to develop digital literacy tools that can be broadly used by educators, youth, and parents. Additionally, our research found that youth and adults wanted pointers to trusted resources to be available within apps should a user seek off-platform support.

Addressing the undermining of digital concerns and self-blame in youth help-seeking. A noteworthy yet unsettling finding was the prevalent self-attribution among youth, which substantially intensifies the apprehension surrounding help-seeking. Our investigation unveiled youth wrestling with guilt, feelings of betrayal, and fear of backlash, particularly in school environments where 'snitching' was stigmatized.

Compounding this issue, we identified a disturbing tendency for adults to diminish or disregard digital concerns voiced by youth. This practice not only hinders the immediate resolution of these issues but also discourages future help-seeking efforts by implicitly trivializing these concerns. This important observation highlights the pressing need to transform how these issues are acknowledged and managed to avoid further disenfranchisement of the already vulnerable. This observation further underscores the nuances of the help-seeking in response to digital abuse experiences and highlights the need for trauma-informed, youth-centered interventions for effective support.

Our study also shed light on fear among youth that consider reporting digital abuse. The anticipation of severe reactions or punitive measures from authority figures, including restrictive actions such as curtailing digital access or enforced social isolation, often inhibits youth from reporting digital threats. This insight calls for the urgent need to foster trust and assure privacy and independence in reporting systems to stimulate more proactive help-seeking.

Community perspectives. Community-level influences encompass school policies towards digital abuse, availability, and accessibility of local mental health resources, and the cultural norms around technology use within the community. The extent to which these entities recognize, respond to, and provide support for

cases of digital abuse may significantly impact a youth's likelihood to seek help. We found that, in the case of schools, institutional policies were inconsistent and often did not include communication directly with parents. Additionally, the institutional responses to digital risks and threats at times resulted in perpetuating harm by focusing on punitive measures rather than educational interventions pertaining to digital safety education. Moving forward research should explore how different approaches taken by schools to address digital abuse impact youth and their families. Additionally, schools can engage more broadly in providing consistent digital safety education through high school to consistently address the different risks and harms youth encounter across different platforms and spaces[61].

Inclusive and adaptable digital safety solutions for youth. Our findings highlight that protecting youth in digital spaces extends beyond individual accountability, consistent with both ecological [233] and communal coping frameworks [143]. Our research emphasizes that the task of safeguarding young people in digital realms goes beyond just holding individuals responsible; it demands the collective efforts of a broad range of stakeholders including parents, advocates, educators, tech industry professionals, policymakers, and community groups. Our findings illuminate the complex sociotechnical dynamics that youth navigate when they engage in help-seeking behaviors in response to digital threats.

However, there is not a one-size-fits-all solution; we need to consider the unique threats that youth face in the digital world [78]. Different individuals may encounter the same threat, but their reactions and the type of support they need can greatly differ. Factors such as the distance to the attacker, past experiences with digital abuse, available support networks, and their own proficiency and

comfort with navigating the digital help-seeking landscape all play significant roles in these differences. Therefore, our research underscores that the efficacy of digital safety measures does not solely rely on their design, but also on their adaptability to the unique needs of the individual and the help-seeking resources required. Our findings point to the need to include youth as active participants in the co-design of digital safety solutions, expanding prior work [78, 5, 22, 23, 52, 157].

There is also an increasing interest in the development of technology-based interventions to support youth who have experienced digital harm. For instance, some studies have explored the use of chatbots and artificial intelligence (AI) to provide immediate, anonymous support to victims of cyberbullying [182, 205, 235, 163]. These interventions offer promising avenues for enhancing help-seeking and providing immediate support for digital harm, although further research is needed to evaluate their efficacy and accessibility for diverse groups of young people.

Overall, our research contributes insights into the barriers and facilitators of help-seeking behavior among youth facing digital abuse. By identifying the gaps and complexities in the support ecosystem, we provide guidance for designing better tools and interventions to promote help-seeking, enhance digital safety, and support the well-being of youth.

4.5.2 A framework for youth digital help-seeking

In the pursuit of creating more comprehensive and effective strategies to combat digital abuse among youth, we provide a proposed framework for digital help-

seeking based on our data from youth and adult participants, and view this through the lens of the ecological support [233] and the communal coping models [143]. This builds upon Rickwood's four stages of help-seeking behavior [193, 194]. This framework takes into account the larger help-seeking ecosystem, rather than focusing on a single platform or specific support source. By doing so, we aim to address the social and contextual dynamics of help-seeking behaviors, the dynamic interaction between different support resources, and their relationship to various types of digital risks and harms. This study extends the boundaries of ecological [233] and communal coping theories [143] to encompass scenarios of digital abuse, providing ways forward to meet the needs and objectives of individuals facing digital abuse situations. This framework takes into account the multidimensional challenges faced by youth and aims to provide youth-centered support that aligns with their needs and goals.

The PROTECT Framework for Youth Digital Safety includes categorizations that group together key elements of help-seeking to address youth digital risks and harms: *Problem Recognition*, where youth become aware of potential online issues; *Reaching Out*, where they decide to seek assistance; *Organizing Support*, which involves identifying and engaging support systems; *Training in Digital Literacy*, to educate on safe online practices; *Engaging Professionals*, for appropriate professional help; *Continuous Support*, to provide ongoing assistance; and *Tackling Safety Measures*, which involves implementing, evaluating, and adapting monitoring and safety measures, as well as handling evolving situations.

Youth Digital Safety Recommendations:

1. **Awareness/Reaching Out:** Youth are encouraged to identify various forms of abuse - digital, physical, emotional, financial, or otherwise. Digital

literacy for youth and parents on how to identify different types of abuse and recognize their telltale signs

2. **Decision to Seek Help:** Once the abuse is recognized, youth decide to seek help or may be connect to support. The environment in which they communicate their concerns should be trauma-informed, validating, and non-judgmental, thus ensuring that no fear of consequences is experienced.
3. **Identifying and Engaging Support Systems:** Youth identify and actively engage with their immediate support networks. These networks should have privacy protections in place to ensure the safety of the youth.
4. **Digital Literacy and Safety Education:** The process should involve educating both youth and their support systems about safe navigation of digital platforms, how to document evidence of abuse, and the most effective way to report such incidents.
5. **Finding and Accessing Appropriate Professional Help:** This step involves identifying and reaching out to relevant formal resources, such as legal, psychological, medical, educational or technology experts.
6. **Continuous Support:** This involves anticipating and managing potential consequences after reporting the abuse, and providing continued support, safety planning, and ongoing professional assistance.
7. **Monitoring and Safety Measures:** Youth and their support systems monitor the situation and adjust safety strategies in both digital and physical environments, focusing on maintaining the youth's well-being and safety.
8. **Evaluation and Adaptation:** There should be a continual assessment of the effectiveness of the help-seeking measures and interventions deployed, and modifications should be made to address evolving situations.

By shedding light on the often overlooked nuances of the help-seeking process, this framework can drive the development of effective, context-specific interventions and inspire a broader dialogue on youth online safety. Further research is encouraged to explore the practical application of these principles in the design and development of technology-mediated solutions for digital abuse prevention and intervention.

4.5.3 A holistic approach for addressing youth's help-seeking behaviors

Understanding youth help-seeking behaviors in response to digital threats requires acknowledging that there is no singular or linear pathway. Instead, help-seeking is a multifaceted process, influenced by various factors and channeled through multiple pathways that could be activated concurrently or sequentially. For instance, a youth could turn to self-education, while also engaging peers, family, or tech company security and privacy features or engaging moderators in their journey to address digital abuse. This multitude of pathways suggests that help-seeking is not just a solitary endeavor, but often involves the participation of various stakeholders, including peers, family members, educators, and technology companies. Importantly, the choice of which pathway(s) to engage with may change over time, reflecting the fluidity of the youth's experience in response to digital threats.

Recognizing and understanding these help-seeking pathways, and the influencing factors, allows for a more comprehensive view of youth navigation of digital challenges. It highlights the need to develop flexible, adaptive in-

terventions that are sensitive to the individual and communal needs of youth. This holistic approach can support youth throughout their journey of mitigating digital attacks while recognizing that digital threats can have lingering effects and potentially cross over from the digital to the physical world recognizing the cyclical and multifaceted nature of youth experiences with digital threats.

In this regard communal coping [126] provides a lens to understanding that help-seeking can be a shared endeavor. This form of coping, characterized by a collective acknowledgment of a problem and a joint commitment to tackling it, could encompass actions taken by peer groups, families, and communities. In light of this multiplicity of pathways and the involvement of multiple stakeholders, it becomes apparent that addressing youth's digital safety needs requires a flexible, multi-tiered support system. This system should be capable of accommodating the diverse pathways to help-seeking, and responsive to the evolving dynamics of youth experiences and changing sociotechnical implications of the technology created (e.g., social VR, connected devices).

Our study contributes to the understanding of social support-seeking in the face of digital threats and harms experienced by youth. We offer a framework for digital help-seeking that builds upon the ecological support approach [233] and the communal coping model [143], with an aim to unravel the social and contextual dynamics of help-seeking behaviors. We argue for the importance of aligning responses to digital abuse with the actual needs of the youth affected and emphasize the necessity of timely, trauma-informed support. Through our research, we extend the reach of ecological and communal coping models to include situations of digital abuse, providing new insights to understand the needs of individuals in such situations.

4.6 Conclusion

Our study identified that there is no single pathway by which youth seek help. Instead, we identified eleven pathways (ref:Table 3, Section 4.4.2) that may change based on digital threats or the contextual or relational confounding factors impacting youth.

Future research may explore providing personalized recommendations and guidance tailored to each individual's unique circumstances while navigating digital harms. Additionally, interdisciplinary collaboration between researchers, educators, policy, and technology developers is essential for advancing the field of adolescent online safety. By combining expertise from diverse disciplines, we can develop comprehensive approaches that address the complex challenges of online risks.

This collaboration can lead to the creation of evidence-based guidelines, policies, and technological innovations that support safe and empowering digital environments for teenagers. By working together stakeholders can develop and implement privacy-aware mechanisms and educational programs that empower youth, protect privacy, and foster a safer online environment. This collaborative approach ensures that privacy considerations are taken into account while addressing the needs of vulnerable individuals, specifically youth, facing digital abuse.

CHAPTER 5

DISCUSSION AND CONCLUSION

Digital technologies provide youth with opportunities for building social connections, self-expression, exploring their identity, and learning [40, 33, 192, 234]. Pew Research reports that 95% percent of teenagers have access to a smartphone and 45% report having regular access to devices [15]. Consistent access and exposure to media, including content posted by peers, has resulted in both appropriate and inappropriate sharing of information without an understanding of the consequences or the choices that they make as teenagers may put themselves at risk as they navigate social media [174, 133, 129, 15].

The digital safety of youth presents a critical problem that extends beyond isolated online encounters. Existing research has primarily focused on distinct harms or threats, or singular digital platforms [180, 244, 189, 120, 67, 105]. Yet, the experiences of today's youth are far from siloed; they fluidly navigate between digital and physical worlds, confronting a diverse range of threats that traverse digital platforms and potentially seep into their offline lives.

While focusing on individual threats and harms provides meaningful insights into the specific risks young people experience, it does not provide the HCI community with a broad perspective on the range of threats that youth contend with, how they seek or do not seek help in response to these threats, and account for the role of stakeholders in this digital-safety landscape. There has been a call from the HCI community to investigate youth digital-safety experiences to obtain a holistic, contextually relevant understanding that captures the fluid boundaries between their online and offline worlds across multiple platforms and stakeholders taking into account the sociotechnical complexities.

My dissertation investigates youth digital safety experiences in different sociotechnical environments and spaces that encompass help-seeking behavior in response to digital risks and attacks as well as the role of stakeholders within these contexts. The studies in this dissertation describe a broad context of digital-safety threats youth experienced, how different stakeholders conceptualized and managed risk, as well as the shortcomings of both the technology and support systems designed to protect youth. I will first summarize the findings from each study and synthesize the results to describe how this work contributes to the understanding of youth-digital safety.

In the first study (Chapter 2), we interviewed a cross-section of 36 youth (ranging from 10-17 years old) and 65 adult stakeholders across 13 states. The focus was the range of potential threats, attacks, and digital harm that youth are exposed to, and an evaluation of the efficacy of current technology and protective measures employed by stakeholders. The youth in this study described a broad spectrum of digital experiences. Through discussions, we identified several key stakeholders in the digital safety landscape, namely parents, guardians, peers, educators, lawyers, advocates, and law enforcement.

Our work builds on previous research by examining the safety ecosystem from the perspectives of multiple stakeholders. These studies (Chapters 2 and 3) highlight the tensions and conflicts that arise between youth and the multiple stakeholders that provide support. We identify cross-context vulnerabilities to show how youth-experienced digital abuse occurs across multiple accounts and crosses platforms, as well as how these abuse journeys carry over into the physical world. We found that platform features/affordances can present unintended risk for vulnerable youth and that a disparity exists between youth, parents, and

advocates in expectations and perceptions of platform safety (Chapters 2, 3, 4). We illustrate how threats, attackers, and youth can fluidly transition between different platforms, with some threats transcending into the physical world.

We propose that solutions should aim to manage this extensive digital safety environment. This involves enhancing the coordination, communication, alignment, and access to current educational resources for both young people and their supporting adults. We envision our work as a call to arms for other researchers and advocates for youth digital safety. They must study and react to a more comprehensive set of attackers and threats, using a relational approach. Moreover, we stress the importance of providing youth with education and resources to enable youth to safeguard themselves against the myriad of digital threats they encounter.

Our findings emphasize the importance of youth agency in which they are active participants in their own digital safety. Our data showed that youth tended to be treated as objects rather than participants in their own safety in situations in which digital technologies were being used as a protective practice. Currently, controls imposed by schools and parents often operated without consulting the youth involved, leading to perceptions of intrusion or violation of their privacy. As a result, many technologically savvy youth employ various methods such as VPNs, using friends' devices, or disabling features to evade these controls. We emphasize the importance of including youth in the participatory design of protective measures.

For the second study (Chapter 3), we conducted semi-structured interviews with 8 teenagers, 7 parents, and 9 bystanders to understand teenagers' (13-17 yrs of age) experiences with harassment in social virtual reality (social VR)

from the perspectives of various stakeholders. Although prior work has looked at a individual user experiences [35, 81, 208], our work contributes a multi-stakeholder perspective.

Prior work has identified that teenagers are exposed to violence, abuse, sexually explicit content, age-inappropriate content, voice trolling, in social VR [185, 148, 148]. Our research uncovered new forms of harassment in social VR, which stemmed from avatar customization in erotic role-play and abuse through a phenomenon known as phantom sense - an immersive VR-induced experience where a user's brain convinces their body that they are physically experiencing the tactile sensations occurring to their virtual self.

For instance, the process of avatar creation and customization is fraught with its own challenges. Our study found that participants opting to customize their avatars had to resort to third-party software or platforms like Unity or Blender, which lack comprehensive guidelines or mechanisms to regulate the process. Social VR platforms have no control over these third-party entities and offer limited options to filter customized avatars. This leaves users free to create and use avatars that suit their personal needs, inadvertently allowing these avatars to become potential tools of harassment. As a result, the current ecosystem allows users to create and employ avatars that meet their individual requirements, without any checks for safety. There is an opportunity for research to develop guidelines that provide safety recommendations around avatar creation.

Our findings also show that teenagers, bystanders, and parents often perceive and experience the same threats in social VR differently. For instance, while most teenagers consider connecting with strangers in social VR to be an inherent part of the experience, parents and bystanders note potential privacy and security

risks. For instance, our teenage respondents saw establishing relationships with strangers in social VR as a routine part of their experience. On the other hand, the adults we interviewed, whether they were parents or observers, underscored instances where such interactions could compromise a teenager's privacy or security.

Additionally, we observed instances of 'virtual grooming' where a teenage participant was quickly lulled into a sense of trust with a potentially predatory individual. Even when bystanders recognized the situation's potential danger and attempted to intervene, the teenager rebuffed their efforts. This refusal left the teenager more exposed to risks of harassment from the predator. The different perceptions and attitudes towards these situations underscore the complex and sometimes dangerous dynamics in social VR environments.

Social VR lacks universally accepted behavioral standards, leading to potential threats. For example, the absence of age restrictions in a virtual bar could expose teenagers to inappropriate activities. The prevalent sexual symbols in social VR are another example where real-world norms are flouted. These "hidden threats" can easily go unnoticed and should be thoroughly examined in future research.

Moreover, the inherent anonymity of social VR, where avatars mask identities, further complicates the formation of social norms. The nature of social Virtual Reality (VR) allows users to assume any identity they choose through their avatars. This built-in anonymity presents a challenge in setting social norms, as traditional cues for behavior, such as physical appearance or reputation, are obscured. This might enable behavior that would be deemed unacceptable in off-line social settings, contributing to potential risks for youth.

The growth of social VR, although rapid, has not been without its technical limitations. A crucial example is the inadequate availability of moderators, especially in private rooms where safety threats can proliferate. Frequently, the task of moderating these private spaces falls onto the room creators or owners, who may lack the necessary experience to effectively manage such environments, inadvertently making these spaces potential sanctuaries for predators.

Additionally, the very nature of VR technology, providing a solely first-person experience, imposes its own set of limitations. This encapsulated experience has led to a noticeable lack of parental participation in their children's social VR activities. Our study revealed that only a handful of parents engage in social VR activities alongside their children. The absence of features such as ad-hoc recording or browsing history on social VR platforms further exacerbates this issue, making it challenging for teenagers to record their experiences and parents to gain insights into these incidents.

Going forward, we propose design recommendations, recognizing social VR platforms are used by many young people, and suggest an age-matching system to facilitate safer peer interactions. Current age verification methods fall short, prompting us to propose the integration of parental consent during account creation, achieved via a consent form delivered to a parent's phone. While acknowledging potential age misrepresentation, we advocate for ongoing surveillance measures, leveraging algorithms to spot suspicious behavior, ensuring continued accuracy of user age data.

We also suggest a user-friendly "emergency button" feature for social VR platforms, similar to Zoom's screen recording function, that triggers audio and video recording in response to perceived harassment or unsafe incidents. To

prevent misuse, the recorded media should be securely stored locally, accessible only to system moderators, and should also alert parents and moderators immediately when the feature is activated. Given parents' concerns and unfamiliarity with social VR, updating safety education resources to include a VR-specific component could raise awareness of potential risks and empower both parents and teenagers with the knowledge necessary for safe platform use.

In the third study (Chapter 4), drawing from data in Study 1, we identified patterns of help-seeking behaviors in response to digital threats. This research paper highlights the various help-seeking pathways that youth turn to, how their strategies vary based on the digital threats they encounter, perceived or actual risks, and the persistence and severity of such risks. We also describe how security reporting tools do not always align with the help-seeking needs of the youth, and the role of risk behavior and protective practices in their immediate environment in shaping their engagement with support systems. We also expand the boundaries of the ecological support [233] and communal coping [143] models to include digital abuse situations, thus offering new perspectives regarding the needs and goals of individuals in digital abuse situations.

Based on our findings, we propose the PROTECT youth digital safety Framework (Chapter 4) that centers around youth, emphasizing an integrated understanding of the dynamic nature of help-seeking behaviors, the multiplicity of digital harms, and the interactions within the help-seeking ecosystem. As such, it provides a valuable basis for providing support and developing holistic interventions.

The PROTECT Framework for Youth Digital Safety includes *Problem Recognition*, where youth become aware of potential online issues; **Reaching Out**,

where they decide to seek assistance; *Organizing Support*, which involves identifying and engaging support systems; *Training in Digital Literacy* to educate on safe online practices; *Engaging Professionals* for appropriate professional help; *Continuous Support* to provide ongoing assistance; and *Tackling Safety Measures*, which involves implementing, evaluating, and adapting monitoring and safety measures, as well as handling evolving situations.

To expand on this it is important to understand the distinction between *Continuous Support* and *Tackling Safety Measures* within the PROTECT framework. *Continuous Support* acknowledges the necessity of consistent assistance, particularly in guiding youth on safe internet and digital device usage. This includes imparting knowledge on online privacy, crafting strong passwords, maintaining discretion with personal information, and promoting respectful online behavior. Continuous support understands that threats can be persistent, signifying that one-off security measures might not suffice. For example, while blocking or muting addresses immediate concerns, an ongoing approach ensures sustained digital safety.

Tackling Safety Measures highlights that a one-size-fits-all approach to security and privacy does not always capture youth tech safety. This concept applies to the strategies and safeguards put in place to protect young people in the digital world. This could involve implementing parental controls, monitoring online activity, and configuring privacy settings on social media accounts and other online platforms. It also includes continually evaluating these safety measures for effectiveness and adjusting them as needed. For example, as youth grow older, or as new platforms or potential threats emerge, safety measures will need to be adapted. Handling evolving situations is especially important as

digital trends among youth can change rapidly, and new risks can emerge just as quickly.

Our research underscores the necessity of personalized solutions in tackling digital abuse among youth, reflecting the unique threats and varied reactions they experience in the digital-safety landscape. The effectiveness of safety measures depends not only on their design but also on their adaptability to individual needs. Consequently, as prior work has noted, it is vital to include youth as active participants in designing these safety solutions [78, 5, 22, 23, 52, 157].

Our findings highlight (Chapters 2-4) the importance of research exploring youth, digital safety, how manage their digital privacy and security and the importance of recognizing the broader ecosystem of stakeholders that provide support to youth. Through this research we have identified the threats models youth encounter both on digital apps and in social VR (Chapters 2 and 3) and their strategies in seeking help in response to these threat models (Chapter 4).

It is also crucial to recognize that youth are part of broader familial and social structures and their digital safety should be viewed within these contexts. Across all three studies (Chapters 1-3), we take a multi-stakeholder perspective in understanding digital safety noting that adult stakeholders are often presented with challenges in both understanding the technology they were trying to assess for safety and implementing safeguards to protect youth.

Additionally, in Chapter 2, we discuss issues of account impersonation and predatory behavior whereby an adult may appear as a youth using a fake account and/or voice-changing technology. Interestingly, when moving to social VR where the physical presence of an Avatar exists, this can enhance confusion

regarding safety as the avatar's appearance may be made to appear as an adult and create additional risks.

We advocate for an inclusive and context-aware approach to youth digital safety. We need to consider wider social structures, the perspectives of diverse stakeholders, and the unique aspects of the digital environment, such as social virtual reality. By doing so, we can develop strategies that respect and address the diverse experiences and needs of youth, creating safer and more supportive digital environments.

The normalization of potentially risky behaviors by today's youth, like engaging with strangers in social VR and sharing personal images, necessitates a deeper examination. This normalization can perpetuate risks given the duality of these behaviors as they provide social gratification but also present privacy and security threats.

In the context of social VR, (Chapter 3) young individuals often perceive interactions with strangers as an inherent and innocuous part of the virtual experience. This stems from the youth's understanding of social VR as an isolated sphere, separate from their physical existence. However, such a perspective can obscure the reality of potential threats these interactions carry, including cyberbullying and grooming, which can transcend the virtual boundaries and manifest in the physical world.

Similarly, when it comes to sharing intimate images, this practice was described as a social norm (Chapter 2), primarily driven by the promise of trust or intimacy. This act, while seemingly innocent, could lead to serious breaches of privacy, emotional distress, or even more severe implications, such as the

distribution of non-consensual intimate images.

In understanding these challenges, it becomes apparent that solutions should go beyond merely telling youth to avoid strangers online or refrain from sharing intimate images. Instead, we need to foster a nuanced understanding of the implications of such behaviors and the risks they pose. It is crucial to empower the youth with knowledge to allow them to comprehend the potential consequences of their actions fully. In doing so, we can provide them with the necessary tools to navigate digital spaces confidently and safely, thereby addressing the risks introduced by the normalization of these behaviors.

In both social VR (Chapter 3) and digital apps (Chapter 2), our findings highlight how the lack of clear delineation between adult and youth spaces portends significant risks. In social VR, avatars provide adults that have ill-intentions a conduit to craft deceptive identities and to manipulate or expose young users to harmful experiences. Furthermore, the amplified sensation of presence can transform cyberbullying into a more disturbing experience with potentially severe psychological repercussions.

Similarly, social media platforms, with their emphasis on connection and openness, also present specific risks leading to adults impersonating youth, potentially resulting in harmful interactions ranging from online grooming to sextortion and/or extortion Chapter 2. In both social VR and across digital apps, youth shared personal information and moved from an initial platform engagement to another platform sharing additional personal information. This highlights our findings in Chapter 4 that there is no-single help-seeking pathway and that youth will enter the help-seeking ecosystem at different points. We expand upon [193] the conceptual help-seeking model and contribute a framework

that takes into account the multidimensional challenges faced by youth and aims to provide youth-centered support that aligns with their needs and goals.

Creating a safer digital environment is a collaborative effort in which stakeholders implement safeguards, such as age-segregation protocols, enhanced identity verification systems, improved content moderation mechanisms, and accessible parental control options. By adopting a multi-pronged approach, we can better protect youth ecosystem. Our efforts in navigating these challenges will play a significant role in shaping the future of digital safety for our young citizens.

Future research

My past and present work has highlighted that privacy and security needs can be thought of in the context of ecosystems. Many other competing needs, from physical safety to the need for participation in a community, are a part of the privacy and security decisions people make. My future research will continue to address security, privacy, and safety challenges of societal importance, with an emphasis on developing solutions that enhance protection for vulnerable and marginalized populations. I envision that this research can expand into new contexts, user groups, and methodologies.

I am also interested in conducting research on co-designing digital safety and security resources. My ongoing qualitative research has engaged comprehensively with different stakeholders, including youth, parents and caregivers, educators, advocates, and legal professionals, to understand digital risks and harms experienced by youth from varied perspectives. Resources designed for

these groups must be grounded in understanding the sociotechnical complexities inherent to their privacy and security practices and must also be accessible to them. Co-designing with youth and advocates will provide opportunities to design support structures, navigate their security and privacy online, understand their help-seeking behaviors, and listen to their suggestions for how resources could be re-designed. This work will identify recommendations for the HCI and security communities and yield insights that technology companies can explore to create products and policies to meet the needs of vulnerable and marginalized populations.

There is also a need for research on youth digital safety dedicated to designing safer interfaces: Future work could include building and testing prototypes that incorporate intuitive safety features into the design of VR and social media interfaces. For instance, visual cues could be developed to alert users when they might be crossing into potentially unsafe spaces in virtual reality. Participatory design methods, with young users actively involved in the process, would be particularly valuable in creating interfaces that resonate with their experience and needs.

Consequently, an in-depth understanding of how users interact in these anonymized environments becomes critical. By studying how users behave under the cloak of virtual anonymity, we can begin to identify patterns, potential issues, and opportunities for intervention. For instance, are users more likely to engage in harmful behavior when they feel unidentifiable? Are there unique forms of communication or behavior that emerge in VR that we need to address? Do users feel more or less responsible for their actions in VR compared to other digital platforms?

I am interested in also initiating a study to investigate suitable social norms within VR environments. Informed by this research, I can work toward creating guidelines and implement protective measures, ultimately contributing to a healthier and safer VR environment.

Additionally, disabled youth and adults experience digital abuse and face challenges in finding support. My ongoing work has identified how youth with developmental disabilities are at risk for digital abuse. I will investigate the types of digital abuse these populations experience, as well as how families mitigate these threats and implement safety measures. For example, understanding the challenges in digital parenting experienced by deaf parents raising hearing children has been raised as an important issue by advocates in my current research, as these parents may not be able to engage in programming to understand their children's digital lives. Further research is needed to map these threats and protective practices and develop interventions to mitigate these harms.

Conclusion

These proposed research directions could help us better understand specific mechanisms and effective strategies for managing youth digital safety in various contexts. Understanding the intersecting dimensions of privacy, security, and safety within the complex sociotechnical ecosystems of digital interactions is critical to develop effective solutions. Drawing from my research, it is evident that these factors cannot be siloed. They require collaboration and coordination across the ecosystem. My future work will continue to address these interconnected challenges and emphasize the protection of vulnerable and marginalized populations.

My ongoing research underscores the need to understand the digital risks and harms experienced by various stakeholders - including youth, parents, educators, advocates, and legal professionals - from their unique perspectives. Co-designing digital safety resources with youth in collaboration with stakeholders is an approach that allows for inclusivity and accessibility. The outcomes of this comprehensive engagement will inform the design of support structures and resources that are contextually relevant and resonant.

A specific avenue of interest is the development of safer interfaces for emerging technologies such as virtual reality. This requires an in-depth understanding of user behaviors in anonymized environments and a commitment to involving youth in participatory design methods with the aim of integrating intuitive safety features into interfaces to mitigate digital risks and threats.

Moving forward I will continue to focus on safety measures and privacy protections to implement proactive measures into digital interfaces as well as to adjacently work to improve technology policy and educational resources to improve youth digital safety.

BIBLIOGRAPHY

[1] Trauma-Informed Care: A Sociocultural Perspective — ncbi.nlm.nih.gov. https://www.ncbi.nlm.nih.gov/books/NBK207195/. [Accessed 07-Jul-2023].

[2] Trauma-Informed Care (Webpage) — samhsa.gov. https://www.samhsa.gov/resource/dbhis/trauma-informed-care-webpage. [Accessed 07-Jul-2023].

[3] Thanks to our community for making 2018 #vrchat's best year yet! tweet. https://twitter.com/VRChat/status/1086389685268635648, 2019.

[4] Samir Abou El-Seoud, Nadine Farag, and Gerard McKee. A Review on Non-Supervised Approaches for Cyberbullying Detection. *Int. J. Eng. Pedagog.*, 10(4), 2020.

[5] Zainab Agha, Karla Badillo-Urquiola, and Pamela J Wisniewski. " strike at the root": Co-designing real-time social media interventions for adolescent online risk prevention. *Proceedings of the ACM on Human-Computer Interaction*, 7(CSCW1):1–32, 2023.

[6] Mohammed Ali Al-Garadi, Mohammad Rashid Hussain, Nawsher Khan, Ghulam Murtaza, Henry Friday Nweke, Ihsan Ali, Ghulam Mujtaba, Haruna Chiroma, Hasan Ali Khattak, and Abdullah Gani. Predicting Cyberbullying on Social Media in the Big Data Era Using Machine Learning Algorithms: Review of Literature and Open Challenges. *IEEE Access*, 7, 2019.

[7] Dustin Albert, Jason Chein, and Laurence Steinberg. The teenage brain: Peer influences on adolescent decision making. *Current Directions in Psychological Science*, 22(2):114–120, 2013.

[8] Shiza Ali, Afsaneh Razi, Seunghyun Kim, Ashwaq Alsoubai, Joshua Gracie, Munmun De Choudhury, Pamela J Wisniewski, and Gianluca Stringhini. Understanding the digital lives of youth: Analyzing media shared within safe versus unsafe private conversations on instagram. In *CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2022.

[9] Ashwaq Alsoubai, Jihye Song, Afsaneh Razi, Nurun Naher, Munmun De Choudhury, and Pamela J Wisniewski. From'friends with benefits' to'sextortion:'a nuanced investigation of adolescents' online sexual

risk experiences. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2):1–32, 2022.

[10] AltspaceVR. AltspaceVR to Sunset the Platform on March 10, 2023. `https://altvr.com/sunset/`, 2023.

[11] Chintan Amrit, Tim Paauw, Robin Aly, and Miha Lavric. Identifying child abuse through text mining and machine learning. *Expert Systems with Applications*, 88, 2017.

[12] Nazanin Andalibi, Oliver L Haimson, Munmun De Choudhury, and Andrea Forte. Understanding social media disclosures of sexual abuse through the lenses of support seeking and anonymity. In *Proceedings of the 2016 CHI conference on human factors in computing systems*, pages 3906–3918, 2016.

[13] Craig A. Anderson and Brad J. Bushman. Effects of Violent Video Games on Aggressive Behavior, Aggressive Cognition, Aggressive Affect, Physiological Arousal, and Prosocial Behavior: A Meta-Analytic Review of the Scientific Literature. *Psychological Science*, 12, 2001.

[14] Monica Anderson. A majority of teens have experienced some form of cyberbullying. *Pew Research Center*, 2018.

[15] Monica Anderson, Jingjing Jiang, et al. Teens, social media & technology. *Pew Research Center*, 31, 2018.

[16] Apple. Expanded Protections for Children. `https://www.apple.com/child-safety/`, 2023.

[17] Adem Arkadas-Thibert. Article 34: The right to protection from all forms of sexual exploitation and sexual abuse. In *Monitoring State Compliance with the UN Convention on the Rights of the Child*, page 339. Springer, Cham, 2022.

[18] Zahra Ashktorab. A study of cyberbullying detection and mitigation on Instagram. In *ACM Conference on Computer Supported Cooperative Work and Social Computing Companion*, pages 126–130. ACM, 2016.

[19] Zahra Ashktorab and Jessica Vitak. Designing cyberbullying mitigation and prevention solutions through participatory design with teenagers.

In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 3895–3905, 2016.

[20] Kathy Attawell. *Behind the numbers: Ending school violence and bullying*. United Nations Educational, Scientific and Cultural Organization, 2019.

[21] Karla Badillo-Urquiola, Scott Harpin, and Pamela Wisniewski. Abandoned but not forgotten: Providing access while protecting foster youth from online risks. In *Proceedings of the 2017 Conference on Interaction Design and Children*, pages 17–26, 2017.

[22] Karla Badillo-Urquiola, Xinru Page, and Pamela J Wisniewski. Risk vs. restriction: The tension between providing a sense of normalcy and keeping foster teens safe online. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2019.

[23] Karla Badillo-Urquiola, Zachary Shea, Zainab Agha, Irina Lediaeva, and Pamela Wisniewski. Conducting risky research with teens: co-designing for the ethical treatment and protection of adolescents. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW3):1–46, 2021.

[24] Charlene K Baker and Patricia K Carreño. Understanding the role of technology in adolescent dating and dating violence. *Journal of Child and Family Studies*, 25(1):308–320, 2016.

[25] Victoria Banyard, Katie Edwards, Ramona Herrington, Skyler Hopfauf, Briana Simon, and Linda Shroll. Using photovoice to understand and amplify youth voices to prevent sexual and relationship violence. *Journal of Community Psychology*, 50(1):90–110, 2022.

[26] Azy Barak and John M Grohol. Current and future trends in internet-supported mental health interventions. *Journal of Technology in Human Services*, 29(3):155–196, 2011.

[27] Julia Barlińska, Anna Szuster, and Mikołaj Winiewski. Cyberbullying among adolescent bystanders: Role of the communication medium, form of violence, and empathy. *Journal of Community & Applied Social Psychology*, 23(1):37–51, 2013.

[28] Courtney K Barrie, John P Bartkowski, and Timothy Haverda. The digital divide among parents and their emerging adult children: Intergenerational accounts of technologically assisted family communication. *Social Sciences*, 8(3):83, 2019.

[29] Corey H Basch, Lorie Donelle, Joseph Fera, and Christie Jaime. Deconstructing tiktok videos on mental health: cross-sectional, descriptive content analysis. *JMIR formative research*, 6(5):e38340, 2022.

[30] Kathleen C Basile, Heather B Clayton, Sarah DeGue, John W Gilford, Kevin J Vagi, Nicolas A Suarez, Marissa L Zwald, and Richard Lowry. Interpersonal violence victimization among high school students—youth risk behavior survey, united states, 2019. *MMWR Supplements*, 69(1):28, 2020.

[31] Diana Baumrind. A developmental perspective on adolescent risk taking in contemporary america. *New Directions for Child and Adolescent Development*, 1987(37):93–125, 1987.

[32] Paul Best, Elena Gil-Rodriguez, Roger Manktelow, and Brian J Taylor. Seeking help from everyone and no-one: Conceptualizing the online help-seeking process among adolescent males. *Qualitative health research*, 26(8):1067–1077, 2016.

[33] Paul Best, Roger Manktelow, and Brian Taylor. Online communication, social media and adolescent wellbeing: A systematic narrative review. *Children and Youth Services Review*, 41:27–36, 2014.

[34] Frank Biocca and Ben Delaney. Immersive Virtual Reality Technology. *Communication in the Age of Virtual Reality*, 15(32), 1995.

[35] Lindsay Blackwell, Nicole Ellison, Natasha Elliott-Deflo, and Raz Schwartz. Harassment in Social VR: Implications for Design. In *Proc. IEEE VR*, 2019.

[36] Lindsay Blackwell, Emma Gardiner, and Sarita Schoenebeck. Managing expectations: Technology tensions among parents and teens. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, pages 1390–1401, 2016.

[37] Doug A Bowman and Ryan P McMahan. Virtual Reality: How Much Immersion Is Enough? *Computer*, 40(7), 2007.

[38] Danah Boyd. Social network sites as networked publics: Affordances, dynamics, and implications. In *A networked self*, pages 47–66. Routledge, 2010.

[39] Danah Boyd. *It's complicated: The social lives of networked teens*. Yale University Press, 2014.

[40] Danah Boyd. Social media: A phenomenon to be analyzed. *Social Media+ Society*, 1(1):2056305115580148, 2015.

[41] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.

[42] Urie Bronfenbrenner. Toward an experimental ecology of human development. *American psychologist*, 32(7):513, 1977.

[43] Urie Bronfenbrenner et al. Ecological models of human development. *International encyclopedia of education*, 3(2):37–43, 1994.

[44] Angela Browne and David Finkelhor. Impact of Child Sexual Abuse: A Review of the Research. *Psychological Bulletin*, 99(1), 1986.

[45] Emily M Buehler. "you shouldn't use facebook for that": Navigating norm violations while seeking emotional support on facebook. *Social Media+ Society*, 3(3):2056305117733225, 2017.

[46] Xavier V Caddle, Nurun Naher, Zachary P Miller, Karla Badillo-Urquiola, and Pamela J Wisniewski. Duty to respond: The challenges social service providers face when charged with keeping youth safe online. *Proceedings of the ACM on Human-Computer Interaction*, 7(GROUP):1–35, 2023.

[47] Jane EM Callaghan, Joanne H Alexander, Judith Sixsmith, and Lisa Chiara Fellin. Beyond "witnessing": Children's experiences of coercive control in domestic violence and abuse. *Journal of Interpersonal Violence*, 33(10):1551–1581, 2018.

[48] Amy Callahan and Kay Inckle. Cybertherapy or psychobabble? a mixed methods study of online emotional support. *British Journal of Guidance & Counselling*, 40(3):261–278, 2012.

[49] Daniel S Campagna and Donald L Poffenberger. *The sexual trafficking in children: An investigation of the child sex trade*. Auburn House Publishing Company, 1988.

[50] Pamara F Chang and Natalya N Bazarova. Managing stigma: Disclosure-

response communication patterns in pro-anorexic websites. *Health Communication*, 31(2):217–229, 2016.

[51] Pamara F Chang, Janis Whitlock, and Natalya N Bazarova. "to respond or not to respond, that is the question": The decision-making process of providing social support to distressed posters on facebook. *Social Media+ Society*, 4(1):2056305118759290, 2018.

[52] Neeraj Chatlani, Arianna Davis, Karla Badillo-Urquiola, Elizabeth Bonsignore, and Pamela Wisniewski. Teen as research-apprentice: A restorative justice approach for centering adolescents as the authority of their own online safety. *International Journal of Child-Computer Interaction*, 35:100549, 2023.

[53] Larissa S Christensen, Dominique Moritz, and Ashley Pearson. Psychological Perspectives of Virtual Child Sexual Abuse Material. *Sexuality & Culture*, 25(4), 2021.

[54] Fast Company. If the metaverse is the future of social media, teens aren't convinced. `https://www.fastcompany.com/90740073/if-the-metaverse-is-the-future-of-social-media-teens-arent-convinced`, 2022.

[55] Patrick W Corrigan, Amy C Watson, and Leah Barr. The self–stigma of mental illness: Implications for self–esteem and self–efficacy. *Journal of social and clinical psychology*, 25(8):875–884, 2006.

[56] Lorrie Faith Cranor, Adam L Durity, Abigail Marsh, and Blase Ur. Parents' and Teens' Perspectives on Privacy In a Technology-Filled World. In *Proc. SOUPS*, 2014.

[57] Olivia Cullen, Keri Zug Ernst, Natalie Dawes, Warren Binford, and Gina Dimitropoulos. "our laws have not caught up with the technology": Understanding challenges and facilitators in investigating and prosecuting child sexual abuse materials in the united states. *Laws*, 9(4):28, 2020.

[58] Elmira Deldari, Diana Freed, and Yaxing Yao. Supporting a safe and healthy immersive environment for teenagers. *UMBC Student Collection*, 2022.

[59] Michael A DeVito, Ashley Marie Walker, and Jeremy Birnholtz. 'too gay for facebook' presenting lgbtq+ identity throughout the personal social

media ecosystem. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):1–23, 2018.

[60] Michele Di Capua, Emanuel Di Nardo, and Alfredo Petrosino. Unsupervised Cyber Bullying Detection in Social Networks. In *Proc. ICPR*, 2016.

[61] Dominic DiFranzo, Yoon Hyung Choi, Amanda Purington, Jessie G Taft, Janis Whitlock, and Natalya N Bazarova. Social media testdrive: Real-world social media education for the next generation. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–11, 2019.

[62] Dominic DiFranzo, Samuel Hardman Taylor, Franccesca Kazerooni, Olivia D Wherry, and Natalya N Bazarova. Upstanding by Design: Bystander Intervention in Cyberbullying. In *Proc. CHI*, 2018.

[63] Stefan C Dombrowski, John W LeMasney, C Emmanuel Ahia, and Shannon A Dickson. Protecting children from online sexual predators: technological, psychoeducational, and legal considerations. *Professional Psychology: Research and Practice*, 35(1):65, 2004.

[64] Diana M Doumas and Aida Midgett. Witnessing cyberbullying and suicidal ideation among middle school students. *Psychology in the Schools*, 60(4):1149–1163, 2023.

[65] Claire Burke Draucker and Donna S Martsolf. The role of electronic communication technology in adolescent dating violence. *Journal of Child and Adolescent Psychiatric Nursing*, 23(3):133–142, 2010.

[66] Matthew S Eastin and Robert P Griffiths. Beyond the Shooter Game: Examining Presence and Hostile Outcomes Among Male Game Players. *Communication Research*, 33(6), 2006.

[67] Anandi C Ehman and Alan M Gross. Sexual cyberbullying: review, critique, & future directions. *Aggression and violent behavior*, 44:80–87, 2019.

[68] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *Proc. CHI*, 2019.

[69] Marie Eneman, Alisdair A Gillespie, and C Stahl Bernd. Technology and

Sexual Abuse: A Critical Review of an Internet Grooming Case. In *Proc. ICIS*, 2010.

[70] Elizabeth Englander. Coerced sexting and revenge porn among teens. *Bullying, Teen Aggression & Social Media*, 1(2):19–21, 2015.

[71] Erik H Erikson. *Identity youth and crisis*. Number 7. WW Norton & company, 1968.

[72] Erik H Erikson. *Childhood and society*. WW Norton & Company, 1993.

[73] Samuel Farley, Iain Coyne, and Premilla D'Cruz. Cyberbullying at work: Understanding the influence of technology. *Concepts, Approaches and Methods*, 2021.

[74] David Finkelhor, Heather Turner, and Deirdre Colburn. Prevalence of online sexual offenses against children in the us. *JAMA network open*, 5(10):e2234471–e2234471, 2022.

[75] Benjamin W Fisher, Joseph H Gardella, and Abbie R Teurbe-Tolon. Peer cybervictimization among adolescents and the associated internalizing and externalizing problems: A meta-analysis. *Journal of youth and adolescence*, 45:1727–1743, 2016.

[76] Centers for Disease Control, Prevention, et al. Youth risk behavior survey data summary & trends report 2007–2017. 2020.

[77] Elizabeth Foss, Allison Druin, and Mona Leigh Guha. Recruiting and retaining young participants: Strategies from five years of field research. In *Proceedings of the 12th International Conference on Interaction Design and Children*, pages 313–316, 2013.

[78] Diana Freed, Natalie N Bazarova, Sunny Consolvo, Eunice J Han, Patrick Gage Kelley, Kurt Thomas, and Dan Cosley. Understanding digital-safety experiences of youth in the us. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2023.

[79] Guo Freeman and Dane Acena. Hugging from A Distance: Building Interpersonal Relationships in Social Virtual Reality. In *Proc. ACM IMX*, 2021.

[80] Guo Freeman, Dane Acena, Nathan J McNeese, and Kelsea Schulenberg.

Working Together Apart through Embodiment: Engaging in Everyday Collaborative Activities in Social Virtual Reality. In *Proc. GROUP*, 2022.

[81] Guo Freeman, Samaneh Zamanifard, Divine Maloney, and Dane Acena. Disturbing the Peace: Experiencing and Mitigating Emerging Harassment in Social Virtual Reality. In *Proc. CSCW1*, 2022.

[82] Guo Freeman, Samaneh Zamanifard, Divine Maloney, and Alexandra Adkins. My Body, My Avatar: How People Perceive Their Avatars in Social Virtual Reality. In *Extended Abstracts of CHI*, 2020.

[83] James Garbarino and Ann Crouter. Defining the community context for parent-child relations: The correlates of child maltreatment. *Child development*, pages 604–616, 1978.

[84] Philip Gillingham. Predictive Risk Modelling to Prevent Child Maltreatment and Other Adverse Outcomes for Service Users: Inside the 'Black Box' of Machine Learning. *The British Journal of Social Work*, 46(4), 2016.

[85] Google. Fighting child sexual abuse online. `https://protectingchildren.google/`, 2022.

[86] William R Graham Jr. Uncovering and Eliminating Child Pornography Rings on the Internet: Issues regarding and Avenues Facilitating Law Enforcement's Access to Wonderland. *L. Rev. MSU-DCL*, 2000.

[87] Amelia Gulliver, Kathleen M Griffiths, and Helen Christensen. Perceived barriers and facilitators to mental health help-seeking in young people: a systematic review. *BMC psychiatry*, 10(1):113, 2010.

[88] Stephen M Haas, Meghan E Irr, Nancy A Jennings, and Lisa M Wagner. Communicating thin: A grounded model of online negative enabling support groups in the pro-anorexia movement. *new media & society*, 13(1):40–57, 2011.

[89] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. "It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *Proc. CHI*, 2020.

[90] Byron Hall and David Dryden Henningsen. Social facilitation and human–computer interaction. *Computers in human behavior*, 24(6):2965–2971, 2008.

[91] Catherine Hamilton-Giachritsis, Elly Hanson, Helen Whittle, Filipa Alves-Costa, and Anthony Beech. Technology assisted child sexual abuse in the UK: Young people's views on the impact of online sexual abuse. *Children and Youth Services Review*, 119, 2020.

[92] Catherine Hamilton-Giachritsis, Elly Hanson, Helen Whittle, Filipa Alves-Costa, Andrea Pintos, Theo Metcalf, and Anthony Beech. Technology assisted child sexual abuse: Professionals' perceptions of risk and impact on children and young people. *Child abuse & neglect*, 119, 2021.

[93] Heidi Hartikainen, Netta Iivari, and Marianne Kinnula. Should we design for control, trust or involvement? a discourses survey about children's online safety. In *Proceedings of the The 15th International Conference on Interaction Design and Children*, pages 367–378, 2016.

[94] Heidi Hartikainen, Afsaneh Razi, and Pamela Wisniewski. Safe sexting: The advice and support adolescents receive from peers regarding online sexual risks. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1):1–31, 2021.

[95] Heidi Hartikainen, Afsaneh Razi, and Pamela Wisniewski. 'if you care about me, you'll send me a pic'-examining the role of peer pressure in adolescent sexting. In *Companion Publication of the 2021 Conference on Computer Supported Cooperative Work and Social Computing*, pages 67–71, 2021.

[96] Tyler Hatchel, Cagil Torgal, America J El Sheikh, Luz E Robinson, Alberto Valido, and Dorothy L Espelage. Lgbtq youth and digital media: online risks. In *Child and Adolescent Online Risk Exposure*, pages 303–325. Elsevier, 2021.

[97] Per Moum Hellevik. Teenagers' personal accounts of experiences with digital intimate partner violence and abuse. *Computers in Human Behavior*, 92:178–187, 2019.

[98] Lisa Hellström and Linda Beckman. Life challenges and barriers to help seeking: Adolescents' and young adults' voices of mental health. *International journal of environmental research and public health*, 18(24):13101, 2021.

[99] Nicola Henry, Asher Flynn, and Anastasia Powell. Image-based sexual abuse: Victims and perpetrators. *Trends and Issues in Crime and Criminal Justice*, (572):1–19, 2019.

[100] Emily Herry and Kelly Lynn Mulvey. Gender-based cyberbullying: Understanding expected bystander behavior online. *Journal of Social Issues*, 2022.

[101] Sameer Hinduja and Justin W Patchin. Bullying, cyberbullying, and suicide. *Archives of Suicide Research*, 14(3):206–221, 2010.

[102] Sameer Hinduja and Justin W Patchin. Digital dating abuse among a national sample of us youth. *Journal of Interpersonal Violence*, 36(23-24):11088–11108, 2021.

[103] Sameer Hinduja and Justin W Patchin. Bias-based cyberbullying among early adolescents: Associations with cognitive and affective empathy. *The Journal of Early Adolescence*, page 02724316221088757, 2022.

[104] Shirley Ho, May O Lwin, Liang Chen, and Minyi Chen. Development and validation of a parental social media mediation scale across child and parent samples. *Internet Research*, 30(2):677–694, 2020.

[105] John R Honan. Teens vulnerable to online shopping scams, studies say. 2021.

[106] Jina Huh-Yoo, Afsaneh Razi, Diep N Nguyen, Sampada Regmi, and Pamela J Wisniewski. "help me:" examining youth's private pleas for support and the responses received from peers via instagram direct messages. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2023.

[107] Carrie James, Emily Weinstein, and Kelly Mendoza. Teaching digital citizens in today's world: Research and insights behind the common sense k–12 digital citizenship curriculum. *Common Sense Media*, 2019.

[108] David R Jezl, Christian E Molidor, and Tracy L Wright. Physical, sexual and psychological abuse in high school dating relationships: Prevalence rates and self-esteem issues. *Child and Adolescent Social Work Journal*, 13(1):69–87, 1996.

[109] Haiyan Jia, Pamela J Wisniewski, Heng Xu, Mary Beth Rosson, and John M Carroll. Risk-taking as a learning process for shaping teen's online information privacy behaviors. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, pages 583–599, 2015.

[110] Sara B Johnson, Robert W Blum, and Jay N Giedd. Adolescent maturity and the brain: the promise and pitfalls of neuroscience research in adolescent health policy. *Journal of adolescent health*, 45(3):216–221, 2009.

[111] Lisa M Jones, Kimberly J Mitchell, and David Finkelhor. Trends in youth internet victimization: Findings from three youth internet safety surveys 2000–2010. *Journal of Adolescent Health*, 50(2):179–186, 2012.

[112] Jaana Juvonen and Sandra Graham. Bullying in schools: The power of bullies and the plight of victims. *Annual review of psychology*, 65:159–185, 2014.

[113] Sylvia D Kauer, Cheryl Mangan, and Lena Sanci. Do online mental health services improve help-seeking for young people? a systematic review. *Journal of Medical Internet Research*, 16(3):e66, 2014.

[114] Amro Khasawneh, Kapil Chalil Madathil, Heidi Zinzow, Pamela Wisniewski, Amal Ponathil, Hunter Rogers, Sruthy Agnisarman, Rebecca Roth, and Meera Narasimhan. An investigation of the portrayal of social media challenges on youtube and twitter. *ACM Transactions on Social Computing*, 4(1):1–23, 2021.

[115] Jagdish Khubchandani, Jeffrey Clark, Michael Wiblishauser, Amy Thompson, Cathy Whaley, Rachel Clark, and Jackie Davis. Preventing and responding to teen dating violence: a national study of school principals' perspectives and practices. *Violence and Gender*, 4(4):144–151, 2017.

[116] Seunghyun Kim, Afsaneh Razi, Gianluca Stringhini, Pamela J Wisniewski, and Munmun De Choudhury. You don't know how i feel: Insider-outsider perspective gaps in cyberbullying risk detection. In *ICWSM*, pages 290–302, 2021.

[117] Minsam Ko, Seungwoo Choi, Subin Yang, Joonwon Lee, and Uichin Lee. Familync: facilitating participatory parental mediation of adolescents' smartphone use. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 867–878, 2015.

[118] Robin M Kowalski, Gary W Giumetti, Amber N Schroeder, and Micah R Lattanner. Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, 140(4):1073–1137, 2014.

[119] Robin M Kowalski, Susan P Limber, and Patricia W Agatston. *Cyberbullying: Bullying in the digital age*. John Wiley & Sons, 2012.

[120] Elana R Kriegel, Bojan Lazarevic, Christian E Athanasian, and Ruth L Milanaik. Tiktok, tide pods and tiger king: health implications of trends taking over pediatric populations. *Current Opinion in Pediatrics*, 33(1):170–177, 2021.

[121] Kaylee P Kruzan, Ellen E Fitzsimmons-Craft, Mallory Dobias, Jessica L Schleider, and Abhishek Pratap. Developing, deploying, and evaluating digital mental health interventions in spaces of online help-and information-seeking. *Procedia Computer Science*, 206:6–22, 2022.

[122] Kaylee Payne Kruzan, Natalya N Bazarova, and Janis Whitlock. Investigating self-injury support solicitations and responses on a mobile peer support application. *Proceedings of the ACM on human-computer interaction*, 5(CSCW2):1–23, 2021.

[123] Kaylee Payne Kruzan, Jonah Meyerhoff, Theresa Nguyen, Madhu Reddy, David C Mohr, and Rachel Kornfield. "i wanted to see how bad it was": Online self-screening as a critical transition point among young adults with common mental health conditions. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–16, 2022.

[124] Kaylee Payne Kruzan, Janis Whitlock, and Natalya N Bazarova. Examining the relationship between the use of a mobile peer-support app and self-injury outcomes: longitudinal mixed methods study. *JMIR mental health*, 8(1):e21854, 2021.

[125] Kaylee Payne Kruzan, Janis Whitlock, Natalya N Bazarova, Aparajita Bhandari, and Julia Chapman. Use of a mobile peer support app among young people with nonsuicidal self-injury: small-scale randomized controlled trial. *JMIR formative research*, 6(1):e26526, 2022.

[126] Kaylee Payne Kruzan, Janis Whitlock, Julia Chapman, Aparajita Bhandari, and Natalya Bazarova. Young adults' perceptions of 2 publicly available digital resources for self-injury: Qualitative study of a peer support app and web-based factsheets. *JMIR formative research*, 7(1):e41546, 2023.

[127] Carlo Lai, Gaia Romana Pellicano, Sara Iuliano, Chiara Ciacchella, Daniela Sambucini, Alessandro Gennaro, and Sergio Salvatore. Why people join pro-ana online communities? a psychological textual analysis of eating disorder blog posts. *Computers in Human Behavior*, 124:106922, 2021.

[128] Angela Y Lee and Jeffrey T Hancock. Developing digital resilience: An educational intervention improves elementary students' response to digital challenges. *Computers and Education Open*, page 100144, 2023.

[129] Amanda Lenhart. Teens, social media & technology overview 2015. *Pew Research Center*, 2015.

[130] Sonia Livingstone. Reframing media effects in terms of children's rights in the digital age. *Journal of children and media*, 10(1):4–12, 2016.

[131] Sonia Livingstone, Magdalena Bober, and Ellen J Helsper. Active participation or just more information? young people's take-up of opportunities to act and interact on the internet. *Information, Community & Society*, 8(3):287–314, 2005.

[132] Sonia Livingstone, Leslie Haddon, Anke Görzig, and Kjartan Ólafsson. Risks and safety on the internet: the perspective of european children: full findings and policy implications from the eu kids online survey of 9-16 year olds and their parents in 25 countries. 2011.

[133] Sonia Livingstone and Ellen Helsper. Gradations in digital inclusion: Children, young people and the digital divide. *New media & society*, 9(4):671–696, 2007.

[134] Sonia Livingstone, Lucyna Kirwil, Cristina Ponte, and Elisabeth Staksrud. In their own words: What bothers children online? *European Journal of Communication*, 29(3):271–288, 2014.

[135] Sonia Livingstone and Jessica Mason. Sexual rights and sexual risks among youth online. *London School of Economics and Political Science, commissioned by the European NGO alliance for child safety online (ENACSO)*, 2015.

[136] Sonia Livingstone, Kjartan Ólafsson, Ellen J Helsper, Francisco Lupiáñez-Villanueva, Giuseppe A Veltri, and Frans Folkvord. Maximizing opportunities and minimizing risks for children online: The role of digital skills in emerging strategies of parental mediation. *Journal of Communication*, 67(1):82–105, 2017.

[137] Sonia Livingstone and Peter 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*, 55(6):635–654, 2014.

[138] Sonia Livingstone and Mariya Stoilova. The 4cs: Classifying online risk to children. 2021.

[139] Sonia Livingstone, Mariya Stoilova, Line Indrevoll Stänicke, Reidar Schei Jessen, Richard Graham, Elisabeth Staksrud, and Tine Jensen. Adolescents experiencing internet-related mental health difficulties: the benefits and risks of digital skills. 2022.

[140] Sonia Livingstone, Mariya Stoilova, Line Indrevoll Stänicke, Reidar Schei Jessen, Richard Graham, Elisabeth Staksrud, and Tine Jensen. Young people experiencing internet-related mental health difficulties: the benefits and risks of digital skills. 2022.

[141] Jessica L Lucero, Arlene N Weisz, Joanne Smith-Darden, and Steven M Lucero. Exploring gender differences: Socially interactive technology use/abuse among dating teens. *Affilia*, 29(4):478–491, 2014.

[142] James Lykens, Molly Pilloton, Cara Silva, Emma Schlamm, Kate Wilburn, Emma Pence, et al. Google for sexual relationships: Mixed-methods study on digital flirting and online dating among adolescent youth and young adults. *JMIR Public Health and Surveillance*, 5(2):e10695, 2019.

[143] Renee F Lyons, Kristin D Mickelson, Michael JL Sullivan, and James C Coyne. Coping as a communal process. *Journal of Social and Personal Relationships*, 15(5):579–605, 1998.

[144] Juan M Machimbarrena, Esther Calvete, Liria Fernández-González, Aitor Álvarez-Bardón, Lourdes Álvarez-Fernández, and Joaquín González-Cabrera. Internet Risks: An Overview of Victimization in Cyberbullying, Cyber Dating Abuse, Sexting, Online Grooming and Problematic Internet Use. *International Journal of Environmental Research and Public Health*, 15(11), 2018.

[145] Sheri Madigan, Anh Ly, Christina L Rash, Joris Van Ouytsel, and Jeff R Temple. Prevalence of multiple forms of sexting behavior among youth: A systematic review and meta-analysis. *JAMA pediatrics*, 172(4):327–335, 2018.

[146] Divine Maloney and Guo Freeman. Falling Asleep Together: What Makes Activities in Social Virtual Reality Meaningful to Users. In *Proc. CHI PLAY*, 2020.

[147] Divine Maloney, Guo Freeman, and Andrew Robb. A Virtual Space for All: Exploring Children's Experience in Social Virtual Reality. In *Proc. CHI PLAY*, 2020.

[148] Divine Maloney, Guo Freeman, and Andrew Robb. It Is Complicated: Interacting with Children in Social Virtual Reality. In *Proc. IEEE VRW*, 2020.

[149] Divine Maloney, Guo Freeman, and Andrew Robb. Social virtual reality: ethical considerations and future directions for an emerging research space. In *IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, 2021.

[150] Divine Maloney, Guo Freeman, and Andrew Robb. Stay Connected in An Immersive World: Why Teenagers Engage in Social Virtual Reality. In *Interaction Design and Children*, 2021.

[151] Divine Maloney, Guo Freeman, and Donghee Yvette Wohn. "Talking without A Voice": Understanding Non-Verbal Communication in Social Virtual Reality. In *Proc. CSCW2*, 2020.

[152] Divine Maloney, Samaneh Zamanifard, and Guo Freeman. Anonymity vs. Familiarity: Self-Disclosure and Privacy in Social Virtual Reality. In *Proc. VRST*, 2020.

[153] Giovanna Mascheroni and Kjartan Ólafsson. Net children go mobile: Risks and opportunities. 2014.

[154] KF McCartan and Ruth McAlister. Mobile phone technology and sexual abuse. *Information & Communications Technology Law*, 21(3), 2012.

[155] Darragh McCashin and Colette M Murphy. Using tiktok for public and youth mental health–a systematic review and content analysis. *Clinical Child Psychology and Psychiatry*, 28(1):279–306, 2023.

[156] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. In *Proc. CSCW*, 2019.

[157] Brenna McNally, Priya Kumar, Chelsea Hordatt, Matthew Louis Mauriello, Shalmali Naik, Leyla Norooz, Alazandra Shorter, Evan Golub, and Allison Druin. Co-designing mobile online safety applications with children.

In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–9, 2018.

[158] Joshua McVeigh-Schultz, Anya Kolesnichenko, and Katherine Isbister. Shaping Pro-Social Interaction in VR: An Emerging Design Framework. In *Proc. CHI*, 2019.

[159] Joshua McVeigh-Schultz, Elena Márquez Segura, Nick Merrill, and Katherine Isbister. What's It Mean to "Be Social" in VR?: Mapping the Social VR Design Ecology. In *Proc. DIS*, 2018.

[160] Meta. Parent education hub. `https://www.meta.com/quest/safety-center/parental-supervision/`, 2023.

[161] Microsoft. PhotoDNA. `https://www.microsoft.com/en-us/photodna`, 2022.

[162] Ellen Middaugh, Lynn Schofield Clark, and Parissa J Ballard. Digital media, participatory politics, and positive youth development. *Pediatrics*, 140(Supplement_2):S127–S131, 2017.

[163] Tijana Milosevic, Kanishk Verma, Michael Carter, Samantha Vigil, Derek Laffan, Brian Davis, and James O'Higgins Norman. Effectiveness of artificial intelligence–based cyberbullying interventions from youth perspective. *Social Media+ Society*, 9(1):20563051221147325, 2023.

[164] Kimberly J Mitchell, David Finkelhor, Lisa M Jones, and Janis Wolak. Use of Social Networking Sites in Online Sex Crimes Against Minors: An Examination of National Incidence and Means of Utilization. *Journal of Adolescent Health*, 47(2), 2010.

[165] Kimberly J Mitchell, Lisa M Jones, David Finkelhor, and Janis Wolak. Internet-facilitated commercial sexual exploitation of children: Findings from a nationally representative sample of law enforcement agencies in the united states. *Sexual Abuse*, 23(1):43–71, 2011.

[166] Dan Morse. With children stuck at home during coronavirus shutdowns, online sexual predators can swoop in, Feb 2021.

[167] Amgad Muneer and Suliman Mohamed Fati. A Comparative Analysis of Machine Learning Techniques for Cyberbullying Detection on Twitter. *Future Internet*, 12(11), 2020.

[168] Ashlee Murray. Teen dating violence: Old disease in a new world. *Clinical Pediatric Emergency Medicine*, 20(1):25–37, 2019.

[169] Manja Nikolovska. The Internet as a Creator of a Criminal Mind and Child Vulnerabilities in the Cyber Grooming of Children. *JYU dissertations*, 2020.

[170] Annalaura Nocentini, Juan Calmaestra, Anja Schultze-Krumbholz, Herbert Scheithauer, Rosario Ortega, and Ersilia Menesini. Cyberbullying: Labels, behaviours and definition in three european countries. *Journal of Psychologists and Counsellors in Schools*, 20(2):129–142, 2010.

[171] Patricia Núñez-Gómez, Kepa Paul Larrañaga, Celia Rangel, and Félix Ortega-Mohedano. Critical analysis of the risks in the use of the internet and social networks in childhood and adolescence. *Frontiers in psychology*, 12:683384, 2021.

[172] Paul O'Connell, Debra Pepler, and Wendy Craig. Peer involvement in bullying: Insights and challenges for intervention. *Journal of Adolescence*, 22(4):437–452, 1999.

[173] Candice L Odgers and Michaeline R Jensen. Annual research review: Adolescent mental health in the digital age: facts, fears, and future directions. *Journal of Child Psychology and Psychiatry*, 61(3):336–348, 2020.

[174] Gwenn Schurgin O'Keeffe, Kathleen Clarke-Pearson, et al. The impact of social media on children, adolescents, and families. *Pediatrics*, 127(4):800–804, 2011.

[175] Justin W Patchin and Sameer Hinduja. Changes in adolescent online social networking behaviors from 2006 to 2009. *Computers in Human Behavior*, 26(6):1818–1821, 2010.

[176] Justin W Patchin and Sameer Hinduja. *Cyberbullying prevention and response: Expert perspectives*. Routledge, 2012.

[177] Justin W Patchin and Sameer Hinduja. Cyberbullying among adolescents: Implications for empirical research. *Journal of Adolescent Health*, 53(4):431–432, 2013.

[178] Justin W Patchin and Sameer Hinduja. *Bullying today: Bullet points and best practices*. Corwin Press, 2016.

[179] Justin W Patchin and Sameer Hinduja. Cyberbullying among tweens in the united states: prevalence, impact, and helping behaviors. *The Journal of Early Adolescence*, 42(3):414–430, 2022.

[180] Filipa Pereira, Brian H Spitzberg, and Marlene Matos. Cyber-harassment victimization in portugal: Prevalence, fear and help-seeking among adolescents. *Computers in Human Behavior*, 62:136–146, 2016.

[181] Jochen Peter, Patti M Valkenburg, and Alexander P Schouten. Developing a model of adolescent friendship formation on the internet. *CyberPsychology & Behavior*, 8(5):423–430, 2005.

[182] Lara Schibelsky Godoy Piccolo, Pinelopi Troullinou, and Harith Alani. Chatbots to support children in coping with online threats: Socio-technical requirements. In *Designing Interactive Systems Conference 2021*, pages 1504–1517, 2021.

[183] Claudette Pretorius, Derek Chambers, and David Coyle. Young people's online help-seeking and mental health difficulties: Systematic narrative review. *Journal of medical Internet research*, 21(11):e13873, 2019.

[184] Claudette Pretorius, Darragh McCashin, and David Coyle. Mental health professionals as influencers on tiktok and instagram: What role do they play in mental health literacy and help-seeking? *Internet Interventions*, 30:100591, 2022.

[185] Zheng Qingxiao, Guo Freeman, and Andrew Robb. Understanding Safety Risks and Safety Design in Social VR Environments. In *Proc. CSCW1*, 2023.

[186] Ethel Quayle. Researching online child sexual exploitation and abuse: Are there links between online and offline vulnerabilities? *LSE Research Online Documents on Economics*, 2016.

[187] Ethel Quayle and Max Taylor. Social networking as a nexus for engagement and exploitation of young people. *Information Security Technical Report*, 16(2), 2011.

[188] Cirenia Quintana-Orts, Lourdes Rey, and Félix Neto. Beyond cyberbullying: Investigating when and how cybervictimization predicts suicidal ideation. *Journal of interpersonal violence*, 37(1-2):935–957, 2022.

[189] Afsaneh Razi, Karla Badillo-Urquiola, and Pamela J Wisniewski. Let's talk

about sext: How adolescents seek support and advice about their online sexual experiences. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2020.

[190] Mina Razi, Michelene Chi, and Young Ji Hong. Supporting victims of cyberbullying: A study of online peer support communities. In *Proceedings of the ACM on Human-Computer Interaction*, volume 4, pages 1–24. ACM, 2020.

[191] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. Where is the digital divide? a survey of security, privacy, and socioeconomics. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 931–936, 2017.

[192] Dana Reid and Paul Weigle. Social media use among adolescents: Benefits and risks. *Adolescent Psychiatry*, 4(2):73–80, 2014.

[193] Debra Rickwood, Frank P Deane, Coralie J Wilson, and Joseph Ciarrochi. Young people's help-seeking for mental health problems. *Australian e-Journal for the Advancement of Mental Health*, 4(3):218–251, 2005.

[194] Debra Rickwood, Kerry Thomas, and Sally Bradford. Help-seeking measures in mental health: a rapid review. *Sax Inst*, 1:35, 2012.

[195] Erin Romanchych. *Violent Video Gaming, Parent and Child Risk Factors, and Aggression in School-Age Children*. PhD thesis, University of Windsor (Canada), 2018.

[196] Rec Room. A Parent's Guide to Rec Room. `https://recroom.com/parents-guide`, 2023.

[197] Heidi Adams Rueda, Megan Lindsay, and Lela Rankin Williams. "she posted it on facebook" mexican american adolescents' experiences with technology and romantic relationship conflict. *Journal of Adolescent Research*, 30(4):419–445, 2015.

[198] Tara L Rutkowski, Heidi Hartikainen, Kirsten E Richards, and Pamela J Wisniewski. Family communication: Examining the differing perceptions of parents and teens regarding online safety communication. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–23, 2021.

[199] Semiu Salawu, Yulan He, and Joanna Lumsden. Approaches to Auto-

mated Detection of Cyberbullying: A Survey. *IEEE Transactions on Affective Computing*, 11(1), 2017.

[200] Kavous Salehzadeh Niksirat, Evanne Anthoine-Milhomme, Samuel Randin, Kévin Huguenin, and Mauro Cherubini. "i thought you were okay": Participatory design with young adults to fight multiparty privacy conflicts in online social networks. In *Designing Interactive Systems Conference 2021*, pages 104–124, 2021.

[201] Shruti Sannon, Elizabeth L Murnane, Natalya N Bazarova, and Geri Gay. " i was really, really nervous posting it" communicating about invisible chronic illnesses across social media platforms. In *Proceedings of the 2019 CHI conference on human factors in computing systems*, pages 1–13, 2019.

[202] Gökçe Nur Say, Zehra Babadağı, Koray Karabekiroğlu, Murat Yüce, and Seher Akbaş. Abuse Characteristics and Psychiatric Consequences Associated with Online Sexual Abuse. *Cyberpsychology, Behavior, and Social Networking*, 18(6), 2015.

[203] Morgan Klaus Scheuerman, Stacy M Branham, and Foad Hamidi. Safe spaces and safe places: Unpacking technology-mediated experiences of safety and harm with transgender people. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):1–27, 2018.

[204] Nina Schnyder, Radoslaw Panczak, Nicola Groth, and Frauke Schultze-Lutter. Association between mental health-related stigma and active help-seeking: systematic review and meta-analysis. *The British Journal of Psychiatry*, 210(4):261–268, 2017.

[205] V Selvi, S Saranya, K Chidida, and R Abarna. Chatbot and bullyfree chat. In *2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)*, pages 1–5. IEEE, 2019.

[206] Emily Setty, Jessica Ringrose, and Kaitlyn Regehr. Digital sexual violence and the gendered constraints of consent in youth image sharing. *Rape: A Challenge to Contemporary Thinking—10 Years On; Horvarth, M., Brown, J., Eds*, 2022.

[207] Pavica Sheldon. The relationship between unwillingness-to-communicate and students' facebook use. *Journal of Media Psychology: Theories, Methods, and Applications*, 20(2):67, 2008.

[208] Ketaki Shriram and Raz Schwartz. All Are Welcome: Using VR Ethnography to Explore Harassment Behavior in Immersive Social Virtual Reality. In *Proc. IEEE VR*, 2017.

[209] Del Siegle. Cyberbullying and Sexting: Technology Abuses of the 21st Century. *Gifted Child Today*, 33(2), 2010.

[210] Mel Slater and Maria V Sanchez-Vives. Enhancing Our Lives with Immersive Virtual Reality. *Frontiers in Robotics and AI*, 3, 2016.

[211] Peter K Smith and Sonia Livingstone. Child users of online and mobile technologies–risks, harms and intervention. *Child Psychology and Psychiatry: Frameworks for Clinical Training and Practice*, pages 141–148, 2017.

[212] Laurence Steinberg. Risk taking in adolescence: what changes, and why? *Annals of the New York Academy of Sciences*, 1021(1):51–58, 2004.

[213] Mariya Stoilova, Sonia Livingstone, Rana Khazbak, et al. Investigating risks and opportunities for children in a digital world: A rapid review of the evidence on children's internet use and outcomes. *Innocenti Discussion Paper 2020-03. UNICEF Office of Research – Innocenti, Florence.*, 2021.

[214] Karlie E Stonard. Technology-assisted adolescent dating violence and abuse: A factor analysis of the nature of electronic communication technology used across twelve types of abusive and controlling behaviour. *Journal of Child and Family Studies*, 28(1):105–115, 2019.

[215] Karlie E Stonard. "technology was designed for this": Adolescents' perceptions of the role and impact of the use of technology in cyber dating violence. *Computers in Human Behavior*, 105:106211, 2020.

[216] Karlie E Stonard. The prevalence and overlap of technology-assisted and offline adolescent dating violence. *Current Psychology*, 40(3):1056–1070, 2021.

[217] Karlie E Stonard, Erica Bowen, Kate Walker, and Shelley A Price. "they'll always find a way to get to you": Technology use in adolescent romantic relationships and its role in dating violence and abuse. *Journal of Interpersonal Violence*, 32(14):2083–2117, 2017.

[218] Jack Summers. Nysp warning parents of online 'catfishing' scams targeting teens, Apr 2021.

[219] Magdalena Szumilas and Stan Kutcher. Teen suicide information on the internet: a systematic analysis of quality. *The Canadian Journal of Psychiatry*, 54(9):596–604, 2009.

[220] Margaret Talbot. The attorney fighting revenge porn. *The New Yorker*, 2016.

[221] Lauren C Taylor, Kelsie Belan, Munmun De Choudhury, and Eric PS Baumer. Misfires, missed data, misaligned treatment: Disconnects in collaborative treatment of eating disorders. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1):1–28, 2021.

[222] Coen Teunissen and Sarah Napier. Child sexual abuse material and end-to-end encryption on social media platforms: An overview. *Trends and Issues in Crime and Criminal Justice*, 2022.

[223] Thorn. *(Responding to Online Threats: Minors' Perspective on Disclosing, Reporting, and Blocking)*.

[224] Elyse J Thulin, Marc A Zimmerman, Yasamin Kusunoki, Poco Kernsmith, Joanne Smith-Darden, and Justin E Heinze. Electronic teen dating violence curves by age. *Journal of youth and adolescence*, 51(1):45–61, 2022.

[225] Navandeep Thumber and Prerana Bhandari. Empowering without misinforming adolescents and young adults with cystic fibrosis. comment on "perceptions of social media use to augment health care among adolescents and young adults with cystic fibrosis: Survey study". *JMIR Pediatrics and Parenting*, 5(2), 2022.

[226] Robert S Tokunaga and Krystyna S Aune. Cyber-defense: A taxonomy of tactics for managing cyberstalking. *Journal of interpersonal violence*, 32(10):1451–1475, 2017.

[227] Patrick Tolan and Nancy Guerra. What works in reducing adolescent violence. *Boulder, CO: The Center for the Study and Prevention of Violence*, 1994.

[228] Deborah L Tolman and Sara I McClelland. Normative sexuality development in adolescence: A decade in review, 2000–2009. *Journal of research on adolescence*, 21(1):242–255, 2011.

[229] M Ungar, M Brown, L Liebenberg, R Othman, WM Kwong, M Armstrong,

J Gilgun, F Chaze Brown, D Fuchs, J Lafrance, et al. Resilience related readings. *Development*, 54(4):348–366.

[230] Joris Van Ouytsel, Michel Walrave, Koen Ponnet, An-Sofie Willems, and Melissa Van Dam. Adolescents' perceptions of digital media's potential to elicit jealousy, conflict and monitoring behaviors within romantic relationships. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 13(3):1–21, 2019.

[231] Sofie Vandoninck and Leen d'Haenens. Children's online coping strategies: Rethinking coping typologies in a risk-specific approach. *Journal of adolescence*, 45:225–236, 2015.

[232] Sofie Vandoninck, Leen d'Haenens, and Keith Roe. Online risks: Coping strategies of less resilient children and teenagers across europe. *Journal of children and media*, 7(1):60–78, 2013.

[233] Alan Vaux. An ecological approach to understanding and facilitating social support. *Journal of social and personal relationships*, 7(4):507–518, 1990.

[234] Philippe Verduyn, Oscar Ybarra, Maxime Résibois, John Jonides, and Ethan Kross. Do social network sites enhance or undermine subjective well-being? a critical review. *Social Issues and Policy Review*, 11(1):274–302, 2017.

[235] V Vijayakumar and D Hari Prasad. Intelligent chatbot development for text based cyberbullying prevention. *International Journal of New Innovations in Engineering and Technology*, 17(1):73–81, 2021.

[236] Joyce Vissenberg, Leen d'Haenens, and Sonia Livingstone. Digital literacy and online resilience as facilitators of young people's well-being? *European Psychologist*, 2022.

[237] Emily A Vogels, Risa Gelles-Watnick, and Navid Massarat. Teens, social media and technology 2022. *Pew Research Center*, 2022.

[238] Piper Vornholt and Munmun De Choudhury. Understanding the role of social media–based mental health support among college students: Survey and semistructured interviews. *JMIR Mental Health*, 8(7):e24512, 2021.

[239] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya

Sleeper, and Kurt Thomas. Sok: A framework for unifying at-risk user research. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2022.

[240] Mark West, Rebecca Kraut, and Han Ei Chew. I'd blush if i could: closing gender divides in digital skills through education. 2019.

[241] Pamela Wisniewski. The privacy paradox of adolescent online safety: A matter of risk prevention or risk resilience? *IEEE Security & Privacy*, 16(2):86–90, 2018.

[242] Pamela Wisniewski, Haiyan Jia, Na Wang, Saijing Zheng, Heng Xu, Mary Beth Rosson, and John M Carroll. Resilience mitigates the negative effects of adolescent internet addiction and online risk exposure. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 4029–4038, 2015.

[243] Pamela Wisniewski, Heng Xu, Mary Beth Rosson, and John 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*, pages 523–540, 2017.

[244] Pamela Wisniewski, Heng Xu, Mary Beth Rosson, Daniel F. Perkins, and John M. Carroll. Dear diary: Teens reflect on their weekly online risk experiences. *Conference on Human Factors in Computing Systems - Proceedings*, pages 3919–3930, 2016.

[245] Janis Wolak and David Finkelhor. Sextortion: Findings from a survey of 1,631 victims. 2016.

[246] Janis Wolak, David Finkelhor, Wendy Walsh, and Leah Treitman. Sextortion of minors: Characteristics and dynamics. *Journal of Adolescent Health*, 62(1):72–79, 2018.

[247] Janis Wolak, Kimberly J Mitchell, and David Finkelhor. Does Online Harassment Constitute Bullying? An Exploration of Online Harassment by Known Peers and Online-Only Contacts. *Journal of Adolescent Health*, 41(6), 2007.

[248] Sijia Xiao, Coye Cheshire, and Niloufar Salehi. Sensemaking, support, safety, retribution, transformation: A restorative justice approach to understanding adolescents' needs for addressing online harm. In *CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2022.

[249] Svetlana Yarosh and Stephen Matthew Schueller. "happiness inventors": informing positive computing technologies through participatory design with children. *Journal of medical Internet research*, 19(1):e14, 2017.

[250] Michele L Ybarra and Kimberly J Mitchell. "sexting" and its relation to sexual activity and sexual risk behavior in a national survey of adolescents. *Journal of adolescent health*, 55(6):757–764, 2014.

[251] Kexin Zhang, Elmira Deldari, Zhicong Lu, Yaxing Yao, and Yuhang Zhao. "It's Just Part of Me:" Understanding Avatar Diversity and Self-presentation of People with Disabilities in Social Virtual Reality. In *Proc. ASSETS*, 2022.

[252] Shikun Zhang, Yuanyuan Feng, Yaxing Yao, Lorrie Faith Cranor, and Norman Sadeh. How usable are ios app privacy labels? *UMBC Faculty Collection*, 2022.

[253] Xiaolu Zhang. Charging children with child pornography–Using the legal system to handle the problem of "sexting". *Computer Law & Security Review*, 26(3), 2010.