Understanding Digital-Safety Experiences of Youth in the U.S.

Diana Freed
dlf92@cornell.edu
Cornell University
USA

Natalie N. Bazarova
bazarova@cornell.edu
Cornell University
USA

Sunny Consolvo
sconsolvo@google.com
Google
USA

Eunice Han
eh552@cornell.edu
Cornell University
USA

Patrick Gage Kelley
patrickgage@acm.org
Google
USA

Kurt Thomas
kurtthomas@google.com
Google
USA

Dan Cosley
dcosley@nsf.org
NSF
USA

ABSTRACT

The seamless integration of technology into the lives of youth has raised concerns about their digital safety. While prior work has explored youth experiences with physical, sexual, and emotional threats—such as bullying and trafficking— there is a need for a comprehensive and in-depth understanding of the myriad of threats that youth experience. By synthesizing the perspectives of 36 youth and 65 adult participants from the U.S., we provide an overview of today's complex digital-safety landscape. We describe attacks youth experienced, how these moved across platforms and into the physical world, and the resulting harms. We also describe protective practices the youth and the adults who support them took to prevent, mitigate, and recover from attacks, and key barriers to doing this effectively. Our findings provide a broad perspective to help improve digital safety for youth and to set directions for future work.

KEYWORDS

Digtal safety, youth, teens, security, privacy, abuse

ACM Reference Format:
Diana Freed, Natalie N. Bazarova, Sunny Consolvo, Eunice Han, Patrick Gage Kelley, Kurt Thomas, and Dan Cosley. 2023. Understanding Digital-Safety Experiences of Youth in the U.S.. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23), April 23–28, 2023, Hamburg, Germany*. ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3544548.3581128

CHI '23, April 23–28, 2023, Hamburg, Germany

ACM ISBN 978-1-4503-9421-5/23/04.
https://doi.org/10.1145/3544548.3581128

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 [4, 7, 39], sexual violence [5, 20], dangerous challenges [36, 41], misinformation [75], fraud [31], exposure to dangerous posts and groups [42], and more. The press often raises awareness of threats through attention-grabbing cases like catfishing [72] or sexual predation [52]. 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 [15, 33, 54], and more recent studies addressing how technology may exacerbate these harms [46, 51, 60, 80]. 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 between different threats; and protective practices employed by youth and the adults who support them within the protective ecosystem [67]. Further, although youth online behavior is often studied through secondary analysis of online trace data [23, 24, 38, 60], and youth themselves are sometimes involved through survey [35] and diary methods [2, 81], on balance, youth voices are underrepresented in academic literature regarding digitally-mediated threats [14].

In this paper, we seek to narrow these gaps around including youth voices and providing more comprehensive views of digital

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

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:

- **RQ1: 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 migration 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) [18, 57], 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 part of the digital-safety landscape (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 we believe are important to consider in research, design, and policy efforts to support the digital safety of youth.

2 RELATED WORK

We begin this section with a summary of prior work about the digital habits of youth. We then describe the known threat pathways 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%) [43], over one-third (35%) have a close friend who lives far away, and 15% have a close friend they met online [4]. 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 [77]. Youth also use gaming and financial apps to communicate with others and pursue their interests and independence, and dating apps [50] 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 [12].

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 [48]: (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) [48, 65]. 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 [3]. While digitally-mediated threats can affect anyone, youth are at a disproportionate risk due to their established tendency toward risk-seeking behavior [1, 11, 34, 66, 79] and limited understanding of the consequences of potential threats [78].

Pathways to threats can proliferate due to existing physical world vulnerabilities [48, 55], including unstable living situations, introversion, mental health issues, witnessing or experiencing trauma,

disabilities, and immigrant or refugee status [44, 59, 64]. 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 [55]. 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 [16, 25] as well as how safe spaces can become places where harmful interactions occur for transgender and gender non-conforming people [63].

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. [53], with around 1 in 6 high school students reporting having experienced physical or sexual dating violence [10, 22]. 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 [8, 19, 26, 49, 61, 68–71, 73, 74, 76, 82, 83].

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 [40, 56]. Fifty-nine percent of U.S. teens report having experienced digital harassment or cyberbullying [3], often bias-based cyberbullying targeting individuals based on their social identity, which includes hate speech or gender-based violence [27, 29].

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) [34]. According to Jia et al.'s risk-centric framework [34], 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 [66].

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) [30, 45, 47]. A smaller body of work has focused on youth, engaging them around designs to help youth manage threats like cyberbullying [6] and non-consensual sharing [62], and respond to harms suffered [84].

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 [67].

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).

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.

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 within their school or organization. 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.

[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.
[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.

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 sampling, utilizing referrals from previous participants. All adult participants 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.

3.3 Discussion guides

Discussion guides for both youth and adult participants were structured around our main research questions 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 individual 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 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.

3.4 Data analysis

To analyze our data, we used an inductive thematic analysis [13] 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 4 and Section 5.

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 chose to participate 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 again from the youth at the start of the interview or focus group. 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*

[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.

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

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 our 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 in the included quotes to mitigate identification.

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 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 attempt to compare the 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 these 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.

[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.

4 THREATS EXPERIENCED BY YOUTH

The diverse digital habits and contextual risk factors of our participants led to a complex threat 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. 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.

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.' It makes 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 the 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.

> "Yeah, like 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 *clapback accounts*—single-purpose accounts used in retaliation to say disparaging or otherwise harmful comments about someone in response to 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

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 begin by commenting or liking a video posted by the youth, or requesting 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 would escalate 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 me. Some people 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 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

4.3 Coercive control and 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).

4.4 Unsafe and 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).

Participating in 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.

Purchasing 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 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

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 by giving their child so much access to their personal information is just setting up a dangerous situation for them and their child." – Advocate, P3

4.6 Misinformation and 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

4.7 Summary of attackers and harms

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.

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.

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 login 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, like, super strict parents just raise sneakier children." – Youth, Y80

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 of interactions were concerning, parents might then 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 that 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 in response to parental control. Suspicious or forbidden contacts were given 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.

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.

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

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 to 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

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.

6 DISCUSSION

Together, our findings provide a complex digital-safety threat 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.

6.1 Important 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) [21, 45, 58], 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].

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 relationships: 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.

6.2 Key barriers to effective protective 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

[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.

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 adult stakeholders in the 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 [77]; this made them 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 [37]. 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 [32], while Social Media Test Drive provides youth with guided, simulated social media experiences that support experiential learning around digitally-mediated threats [17]. 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 are not designed to support those needs.

Coordination between stakeholders. 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, describing skepticism, fear, and lack of capability. This makes better reporting features low hanging fruit for helping to improve relationships between stakeholders and mitigate harms.

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. People don't report for the sake of reporting, but are 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 youths' 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 the landscape of platforms and

threats, the resulting practices might be more comprehensive and more tuned to the actual risks youth face around threats, 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 [9, 28].

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 social-economic 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 actors involved in youth digital safety, other opportunities for better managing and mitigating youth safety risks in technologies will arise.

7 CONCLUSION

Through qualitative research with 101 youth and adults who support them, we've provided a complex digital-safety threat 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 this 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 threat 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 attackers 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.

REFERENCES

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

[2] Shiza Ali, Afsaneh Razi, Seunghyun Kim, Ashwaq Alsoubai, Joshua Gracie, Munmun De Choudhury, Pamela J Wisniewski, and Gianluca Stringhini. 2022. 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*. 1–14.

[3] Monica Anderson. 2018. A majority of teens have experienced some form of cyberbullying. *Pew Research Center* (2018).

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

[5] Adem Arkadas-Thibert. 2022. 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*. Springer, Cham, 339.

[6] Zahra Ashktorab and Jessica Vitak. 2016. Designing cyberbullying mitigation and prevention solutions through participatory design with teenagers. In *Proceedings of the 2016 CHI conference on human factors in computing systems*. 3895–3905.

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

[8] Charlene K Baker and Patricia K Carreño. 2016. Understanding the role of technology in adolescent dating and dating violence. *Journal of child and family studies* 25, 1 (2016), 308–320.

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

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

[11] Diana Baumrind. 1987. A developmental perspective on adolescent risk taking in contemporary America. *New directions for child and adolescent development* 1987, 37 (1987), 93–125.

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

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

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

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

[16] Michael A DeVito, Ashley Marie Walker, and Jeremy Birnholtz. 2018. 'Too Gay for Facebook' Presenting LGBTQ+ Identity Throughout the Personal Social Media Ecosystem. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–23.

[17] Dominic DiFranzo, Yoon Hyung Choi, Amanda Purington, Jessie G Taft, Janis Whitlock, and Natalya N Bazarova. 2019. 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*. 1–11. https://doi.org/10.1145/3290605.3300533

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

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

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

[21] Elizabeth Englander. 2015. Coerced sexting and revenge porn among teens. *Bullying, teen aggression & social media* 1, 2 (2015), 19–21.

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

[23] Heidi Hartikainen, Afsaneh Razi, and Pamela Wisniewski. 2021. Safe Sexting: The Advice and Support Adolescents Receive from Peers Regarding Online Sexual Risks. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–31.

[24] Heidi Hartikainen, Afsaneh Razi, and Pamela Wisniewski. 2021. '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*. 67–71.

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

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

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

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

[29] Sameer Hinduja and Justin W Patchin. 2022. Bias-Based Cyberbullying Among Early Adolescents: Associations With Cognitive and Affective Empathy. *The Journal of Early Adolescence* (2022), 02724316221088757.

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

[31] John R Honan. 2021. Teens Vulnerable to Online Shopping Scams, Studies Say. (2021).

[32] Carrie James, Emily Weinstein, and Kelly Mendoza. 2019. Teaching digital citizens in today's world: Research and insights behind the Common Sense K–12 Digital Citizenship Curriculum. *Common Sense Media* (2019).

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

[34] Haiyan Jia, Pamela J Wisniewski, Heng Xu, Mary Beth Rosson, and John M Carroll. 2015. 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*. 583–599.

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

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

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

[38] Seunghyun Kim, Afsaneh Razi, Gianluca Stringhini, Pamela J Wisniewski, and Munmun De Choudhury. 2021. You Don't Know How I Feel: Insider-Outsider Perspective Gaps in Cyberbullying Risk Detection.. In *ICWSM*. 290–302.

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

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

[41] Elana R Kriegel, Bojan Lazarevic, Christian E Athanasian, and Ruth L Milanaik. 2021. TikTok, Tide Pods and Tiger King: health implications of trends taking over pediatric populations. *Current opinion in pediatrics* 33, 1 (2021), 170–177.

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

[43] Amanda Lenhart. 2015. Teens, social media & technology overview 2015. (2015).

[44] Sonia Livingstone, Magdalena Bober, and Ellen J Helsper. 2005. 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 (2005), 287–314.

[45] Sonia Livingstone, Leslie Haddon, Anke Görzig, and Kjartan Ólafsson. 2011. 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).

[46] Sonia Livingstone, Lucyna Kirwil, Cristina Ponte, and Elisabeth Staksrud. 2014. In their own words: What bothers children online? *European Journal of Communication* 29, 3 (2014), 271–288.

[47] Sonia Livingstone, Kjartan Ólafsson, Ellen J Helsper, Francisco Lupiáñez-Villanueva, Giuseppe A Veltri, and Frans Folkvord. 2017. Maximizing opportunities and minimizing risks for children online: The role of digital skills in emerging strategies of parental mediation. *Journal of communication* 67, 1 (2017), 82–105.

[48] Sonia Livingstone and Mariya Stoilova. 2021. The 4Cs: Classifying online risk to children. (2021). https://www.ssoar.info/

[49] Jessica L Lucero, Arlene N Weisz, Joanne Smith-Darden, and Steven M Lucero. 2014. Exploring gender differences: Socially interactive technology use/abuse among dating teens. *Affilia* 29, 4 (2014), 478–491.

[50] James Lykens, Molly Pilloton, Cara Silva, Emma Schlamm, Kate Wilburn, Emma Pence, et al. 2019. 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 (2019), e10695.

[51] Kimberly J Mitchell, Lisa M Jones, David Finkelhor, and Janis Wolak. 2011. 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 (2011), 43–71.

[52] Dan Morse. 2021. With children stuck at home during coronavirus shutdowns, online sexual predators can swoop in. https://www.washingtonpost.com/local/public-safety/coronavirus-lockdown-child-exploitation/2021/02/04/90add6a6-462a-11eb-a277-49a6d1f9dff1_story.html

[53] Ashlee Murray. 2019. Teen Dating Violence: Old Disease in a New World. *Clinical Pediatric Emergency Medicine* 20, 1 (2019), 25–37.

[54] PAUL O'connell, Debra Pepler, and Wendy Craig. 1999. Peer involvement in bullying: Insights and challenges for intervention. *Journal of adolescence* 22, 4 (1999), 437–452.

[55] Candice L Odgers and Michaeline R Jensen. 2020. Annual Research Review: Adolescent mental health in the digital age: facts, fears, and future directions. *Journal of Child Psychology and Psychiatry* 61, 3 (2020), 336–348.

[56] Justin W Patchin and Sameer Hinduja. 2012. *Cyberbullying prevention and response: Expert perspectives*. Routledge.

[57] Justin W Patchin and Sameer Hinduja. 2013. Cyberbullying among adolescents: Implications for empirical research. *Journal of Adolescent Health* 53, 4 (2013), 431–432.

[58] Justin W Patchin and Sameer Hinduja. 2022. Cyberbullying among tweens in the United States: prevalence, impact, and helping behaviors. *The Journal of Early Adolescence* 42, 3 (2022), 414–430.

[59] Jochen Peter, Patti M Valkenburg, and Alexander P Schouten. 2005. Developing a model of adolescent friendship formation on the Internet. *CyberPsychology & Behavior* 8, 5 (2005), 423–430.

[60] Afsaneh Razi, Karla Badillo-Urquiola, and Pamela J Wisniewski. 2020. 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*. 1–13.

[61] Heidi Adams Rueda, Megan Lindsay, and Lela Rankin Williams. 2015. "She posted It on facebook" Mexican American adolescents' experiences with technology and romantic relationship conflict. *Journal of Adolescent Research* 30, 4 (2015), 419–445.

[62] Kavous Salehzadeh Niksirat, Evanne Anthoine-Milhomme, Samuel Randin, Kévin Huguenin, and Mauro Cherubini. 2021. "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*. 104–124.

[63] Morgan Klaus Scheuerman, Stacy M Branham, and Foad Hamidi. 2018. 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 (2018), 1–27.

[64] Pavica Sheldon. 2008. The relationship between unwillingness-to-communicate and students' Facebook use. *Journal of Media Psychology: Theories, Methods, and Applications* 20, 2 (2008), 67.

[65] Peter K Smith and Sonia Livingstone. 2017. Child users of online and mobile technologies–risks, harms and intervention. *Child Psychology and Psychiatry: Frameworks for Clinical Training and Practice* (2017), 141–148.

[66] Laurence Steinberg. 2004. Risk taking in adolescence: what changes, and why? *Annals of the New York Academy of Sciences* 1021, 1 (2004), 51–58.

[67] Mariya Stoilova, Sonia Livingstone, Rana Khazbak, et al. 2021. 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).

[68] Karlie E Stonard. 2019. 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 (2019), 105–115.

[69] Karlie E Stonard. 2020. "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 (2020), 106211.

[70] Karlie E Stonard. 2021. The prevalence and overlap of technology-assisted and offline adolescent dating violence. *Current Psychology* 40, 3 (2021), 1056–1070.

[71] Karlie E Stonard, Erica Bowen, Kate Walker, and Shelley A Price. 2017. "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 (2017), 2083–2117.

[72] Jack Summers. 2021. NYSP warning parents of online 'catfishing' scams targeting teens. https://www.news10.com/news/nysp-warning-parents-of-online-catfishing-scams-targeted-towards-teens-through-social-media

[73] Margaret Talbot. 2016. The attorney fighting revenge porn. *The New Yorker* (2016).

[74] Elyse J Thulin, Marc A Zimmerman, Yasamin Kusunoki, Poco Kernsmith, Joanne Smith-Darden, and Justin E Heinze. 2022. Electronic teen dating violence curves by age. *Journal of youth and adolescence* 51, 1 (2022), 45–61.

[75] Navandeep Thumber and Prerana Bhandari. 2022. 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).

[76] Joris Van Ouytsel, Michel Walrave, Koen Ponnet, An-Sofie Willems, and Melissa Van Dam. 2019. Adolescents' perceptions of digital media's potential to elicit jealousy, conflict and monitoring behaviors within romantic relationships. *Cyberpsychology: journal of psychosocial research on cyberpspace.-Brno* 13, 3 (2019), 1–21.

[77] Emily A Vogels, Risa Gelles-Watnick, and Navid Massarat. 2022. Teens, Social Media and Technology 2022. (2022).

[78] Pamela Wisniewski. 2018. The privacy paradox of adolescent online safety: A matter of risk prevention or risk resilience? *IEEE Security & Privacy* 16, 2 (2018), 86–90.

[79] Pamela Wisniewski, Heng Xu, Mary Beth Rosson, and John M Carroll. 2017. 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*. 523–540.

[80] Pamela Wisniewski, Heng Xu, Mary Beth Rosson, Daniel F. Perkins, and John M. Carroll. 2016. Dear diary: Teens reflect on their weekly online risk experiences. *Conference on Human Factors in Computing Systems - Proceedings* (2016), 3919–3930. https://doi.org/10.1145/2858036.2858317

[81] Pamela Wisniewski, Heng Xu, Mary Beth Rosson, Daniel F Perkins, and John M Carroll. 2016. Dear diary: Teens reflect on their weekly online risk experiences. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 3919–3930.

[82] Janis Wolak and David Finkelhor. 2016. Sextortion: Findings from a survey of 1,631 victims. (2016).

[83] Janis Wolak, David Finkelhor, Wendy Walsh, and Leah Treitman. 2018. Sextortion of minors: Characteristics and dynamics. *Journal of Adolescent Health* 62, 1 (2018), 72–79.

[84] Sijia Xiao, Coye Cheshire, and Niloufar Salehi. 2022. 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*. 1–15.