# Experts' Views on Digital Parenting Strategies

**Abigail Marsh**
Carnegie Mellon University
Pittsburgh, USA
acmarsh@cmu.edu

**Lorrie Faith Cranor**
Carnegie Mellon University
Pittsburgh, USA
lorrie@cmu.edu

**Julie S. Downs**
Carnegie Mellon University
Pittsburgh, USA
downs@cmu.edu

## ABSTRACT
American teenagers are spending much of their time online. Online communities offer teens perspective, acceptance, connection, and education that were once more limited by geography. However, the online world also opens teens to risks. Adults must decide how to guide teen online behavior in a space that they may not understand. We interviewed 16 experts about teen online behavior, related benefits and risks, and risk mitigation methods. We found that experts agree on certain mitigation methods, especially communication and education about online behavior, but are divided over monitoring. We propose a set of possible solutions that promote online safety while preserving teens' privacy.

### Author Keywords
Teenager; Adolescent; Privacy; Risk; Safety; Expert Interviews; Expert Elicitation.

## INTRODUCTION
In our current digital age, American teenagers are spending a large amount of their lives online. The online world brings both enormous opportunities and new risks.

In digital communities, teens learn how to appropriately express themselves, and find resources to learn and grow. Teens explore their identities online. Marginalized groups, like homosexual teens, find accepting communities that help them gain confidence and accept themselves. In addition, the ease of digital communication allows teens to strengthen their social bonds, keep in touch with distant friends and family, and even learn about job and education opportunities.

As with any form of engagement, however, the online world comes with risks. We hear about some of these risks in tragic news stories about cyberbullying and teen suicide. We also hear about less severe risks, such as Tinder promoting hookup culture [25], or how being online encourages unhealthy sleep habits and increases risk of depression [27].

The often conflicting information about the benefits and risks of teen online engagement complicates parents' decisions about how best to keep their kids safe online. Schools, law enforcement, and other parties are also drawn into the discussion of how to address teens' digital behavior. Although it is tempting to monitor everything teens do for any sign of danger, this may leave teens exposed to misinterpretation and feeling violated by adults they should trust, at a time when they are developing their own identity and viewpoints.

In this paper, we investigate experts' views on teens' online activity. We focus primarily on experts' views of the risks and benefits posed to teens, and how parents are attempting to mitigate those risks while promoting healthy online engagement.

We conducted semi-structured interviews with 16 experts in the fields of teen behavior, online privacy, security, cybercrime, and monitoring software. Some of these clinical perspectives are not academically published, but are widely disseminated through seminars or popular media. We believe that presenting this expertise contributes information unlikely to be found in a review of only academic literature.

Experts generally agreed about rules that limit online access around dinner and bedtime and they believed parents should be proactive in discussing teens' online activities. They also felt education and communication about appropriate online behavior were essential.

We found that our expert interviewees were particularly divided over the use of monitoring methods to watch what teens were doing online. Some experts felt that monitoring was an unnecessary privacy invasion for most teens; others felt it was a necessary part of modern parenthood. The experts who supported monitoring generally thought that very harmful online experiences were common for teens, perhaps due to their occupational observation of harms [29], whereas experts disavowing monitoring felt that such outcomes were rare. The discrepancy between expert responses suggests a need for new solutions that offer both online safety and private digital space for teens.

## RELATED WORK
As children get older and enter adolescence, they increasingly engage with social media. Social media is the primary method of communication for many current teens [24], and most teens are online daily [12]. Indeed, boyd [3] writes that, due to restrictions on teens' access to transportation and public spaces, and changing social norms about allowing teens to go out unsupervised, digital means are often the only way for teens to talk to their friends outside of school hours.

As a result of this social migration to the Internet and parents' heightened awareness of the risks their teens face, parents

feel that they must find ways to ensure their teens are safe online [35]. This poses challenges because many teens do not understand online privacy risks [19].

One noted difficulty parents face is finding a balance of parental monitoring and teens' independence: almost all parents feel that their children need on- and offline space to mature as they get older, but they aren't sure how to monitor it [5]. This compounds with natural differences in parenting style [35] and ethical views of monitoring [18], making advice difficult to prescribe.

Though most parents believe that teens have a right to some amount of privacy, previous work has shown that these parents may engage in hypocritical monitoring practices when motivated to protect their teens from risk [21]. Other research has noted that conflict between parents and teens results from disagreements about and different expectations of teens' privacy needs [23, 10]. Although conflict leads to negotiation about teens' privacy rights, some research asserts that mandatory negotiation is damaging, stating "surveillance is a form of oppression" [3].

Currently, the question of parental monitoring practices divides the research community. Although boyd takes a strongly permissive stance in arguing for teens' right to have nearly unburdened privacy, others, including Schoenebeck, sympathize more strongly with parents. In part, this is a result of their research methods—Schoenebeck has studied online parenting groups focused on supporting parents of young children or children with special needs [1, 26]. These children do not have the agency and reasoning power to make online privacy decisions, and research in this area reasonably focuses on parental behaviors [20]. In contrast, boyd has interviewed mostly teens who are capable of reasoning about their online behavior and associated risks [3]; the parents of these teens will generally need far less control of their teens' online identities to mitigate risks. Likely, a balance of these and other monitoring and parenting behaviors will be relevant throughout the spectrum of family dynamics.

Many researchers have observed that parental monitoring causes adolescents to withdraw and share less personal information with their parents [10]. In contrast, when parents and teens have positive relationships with each other, teens willingly discuss personal information and concerns [28]. Strict monitoring can make this positive relationship, trust, and even teens' ability to negotiate for privacy difficult to achieve [13].

Further hampering parent-teen communication are parents' often inaccurate warnings about risky behavior. Despite frequent media scares about sexting, most teens who sext face no negative consequences; one study posits that sexting poses a significant risk primarily to teens who are pressured into it [9]. Parents' dire warnings about sexting may exaggerate the likelihood of negative outcomes compared to the teen's experience, leading teens to ignore even moderate warnings because they believe that the likelihood of all negative outcomes are exaggerated.

Similarly, adults may be concerned about cyberbullying. But Marwick and boyd write that teens define many online conflicts as drama, which they differentiate from bullying as a less serious, even entertaining, act [15]. In a participatory design study, a group of teens even disagreed within themselves about what constituted cyberbullying, dividing along gender lines over whether exclusion was bullying [2]. Approaching "drama" behaviors as bullying might turn teens off of advice, leaving them under-prepared if the behavior escalates.

Marwick et al. [17] note the importance of studying teen privacy in relation to technology, given much of teen socialization is online, and that teens highly value digital privacy. A Pew research report supports Marwick et al.'s finding that teens take active steps to protect their privacy online: 74% of teens had removed people from their friends list, thereby taking control of or limiting their online audience [14].

In further research, Marwick and boyd found that teens used numerous methods to preserve their online privacy. In contrast to adult expectations, teens were not often using privacy settings provided by social networking sites; they instead couched posts in language that could only be understood by the intended audience. They also engaged in risky behaviors, such as password sharing, without believing that this act waived all of their expectations of privacy [16]. These privacy norms may not be obvious to many adults.

Parents often do not appreciate that teens consider their digital activity to be private. In a study by Cranor et al. [5], 8 out of 10 parents interviewed stated that reading their teens' text messages was ethical, yet all of the teens interviewed felt text messages were equivalent to private in-person conversations.

A thorough understanding of teens' technology use can be critical for parents beyond respecting the privacy of text messages. In a study of 12 parent-teen dyads, Wisniewski et al. found that technologically literate parents engaged more actively with their teens' online behaviors. However, they found that less adept parents favored restricting teens' online activity, which may be equivalent to greatly restricting their social interactions, a strategy likely to have negative implications for teens' development [33]. The authors further assert that highly engaged parents may be the most successful at reducing teens' risk while allowing them to socialize online [31].

Some experts suggest that risk exposure can be helpful for teens. Teens who have experienced risk tend to be concerned about privacy and perform more risk-coping behaviors as a reaction [11, 30], and one diary study found that low-risk experiences especially may provide beneficial learning opportunities [32]. Even adults are largely unable to manage unfamiliar risks [8, 7]. By allowing teens to engage with some low-level risks, and educating them rather than punishing them, parents may encourage teens to be more concerned about and involved in protecting teens' own privacy.

In a similar realm, studies have examined how teens understand risky sexual behavior [6]. Here, female teens revealed concerns about risk to be somewhat secondary to the powerful social normative forces driving sexual behavior among teens. The two realms can intersect when sexual behavior goes digital, in the form of sexting [9].

Though many experts turn to fear as a motivator, extensive surveys of the literature on fear appeals suggest that threatening and fear-based communication do not reduce risky behavior [22]. Also, fear appeals may lead people to control their fear about risks by ignoring or denying the risk rather than by coping with the posed threat [34]. In sum, prior research on fear appeals suggests that using fear to motivate teens not to engage in risky behavior may just push them to deny the risks, rather than dissuade the behavior.

## METHODOLOGY

We conducted one-hour semi-structured interviews with 16 expert participants. Our study was approved by the Carnegie Mellon University Institutional Review Board.

### Recruitment and Confidentiality

We recruited our expert participants by invitation. We identified categories from which we sought experts, including: researchers who focus on online privacy, security, and teen behavior; employees of social media companies who work on teen issues; employees of monitoring or online safety software companies; educators who discuss online behavior with teens; and law enforcement officers and analysts who specialize in cybercrimes involving child and teen victims.

We found participants through our prior knowledge of the field, news articles, and recommendations from other experts. We began by contacting professional acquaintances who work in this field, invited them to be interviewed, and asked for suggestions of others to contact. We reviewed recent news articles about teen online privacy and safety, and invited the experts quoted. We told participants that we wished to interview them for a study on teens' risky online behavior. We contacted 27 potential participants, and completed 16 interviews between May and November 2015. Our participants are described in Table 1. For their participation in our one-hour interview, we compensated participants with $25 in Amazon.com credit.

We interviewed four male and twelve female experts, all of whom live in the United States. During the course of the interviews, twelve of our participants mentioned that they had children; the others did not mention parental status. Two experts were PhD candidates; they had both returned to graduate school to pursue second-career interests, and brought knowledge and experience from their first careers into their interviews as well as experience from their PhD research.

We avoided choosing quotes for this paper that would identify any of our experts. We also asked expert participants how they would prefer to specify their job title, and further anonymized them as necessary. Some research suggests that expert participants should not be anonymized in order to properly attribute credit for their work [4]. In this case, we do not discuss our participants' original work, and anonymization has enabled participation from experts who otherwise would have had to seek approval from their employer or censored their responses in order to take part.

### Interview Procedure

We conducted most of our expert interviews with one researcher; for three participants, a research assistant was also present. We began each interview by obtaining consent and explaining the study's purpose. Most of the interviews were conducted remotely, using either the telephone or voice over IP; only two experts were interviewed in person.

Our semi-structured interview script covered teens' online behaviors; risks and harms resulting from their online behaviors; parental restrictions, rule-enforcement, and practices; privacy; and the role of third-parties and software tools.

### Content Coding

The researchers met weekly during and after the interview process to review notes and impressions from the interviews and to identify emerging themes that we would further investigate during our coding process. We collaboratively developed a draft codebook containing 105 codes in 7 categories.

We transcribed our interviews for coding and analysis. One research assistant and one of the authors used our draft codebook to code each of these interviews. We reduced the codebook after this first round of coding, after which the coders then recoded the interviews using the revised codebook. Additional consolidation reduced the codebook to 41 codes in 7 categories. Two additional research assistants and one of the authors then finished coding the interviews. We met again to discuss and reach consensus on our coding.

### Limitations

Our expert participants were not a representative sample of all professionals who deal with teens' online behaviors. However, our experts were recruited from a variety of fields, including law enforcement, education, industry, and academia. Our results capture a wide range of opinions and expertise, providing a multifaceted view of teens' online behavior and the associated outcomes. There may be other, less broadly held perspectives that our interviews did not reveal.

In discussion, expertise sometimes drifted into opinion in a way that mirrored the nature of the expert's perspective on the problem. Rather than attempt to differentiate opinion from expertise and exclude the former category, we retain all statements and attempt to draw inferences about how opinions can evolve differently depending on one's area of expertise.

## HIGH-LEVEL CONCEPTUAL MODEL

In advance of our interviews with experts, we prepared a high-level conceptual model of parents' and teens' actions and perceptions of teen online behavior (Figure 1). We developed this model using our knowledge of related work as well as our prior research. The model reflects that teens' and parents' perspectives play heavily into how they make decisions about online behavior. This model was not shown to participants, but used as a framework through which to understand their responses.

We envision the ground truth of teens' behaviors and outcomes as being directly influenced by teens' own perceptions of their behaviors and outcomes, as well as by *parent interventions* to moderate those behaviors. These interventions may be influenced by teens' behaviors, including communication. But parent interventions may evoke a strategic response from

| Participant | Role | Self-Described Occupation |
|---|---|---|
| E1 | Educator | High school social worker |
| E2 | Educator | Author, attorney, and lecturer |
| E3 | Educator | Teacher |
| I1 | Online industry | Works on safety policies for the technology industry |
| I2 | Online industry | Chief privacy officer |
| L1 | Law professional | Computer crime investigator |
| L2 | Law professional | Privacy lawyer |
| LR1 | Law professional/researcher | PhD candidate, former internet crimes against children analyst |
| P1 | Child protection software industry | Founder of an online privacy and security software company |
| P2 | Child protection software industry | CEO of an online safety software company |
| R1 | Researcher | Cybersecurity education researcher |
| R2 | Researcher | Director of a bullying research center |
| R3 | Researcher | Researcher on children's privacy |
| R4 | Researcher | Academic researcher |
| R5 | Researcher | PhD candidate |
| R6 | Researcher | Researcher |

**Table 1. Occupations of our study participants.**

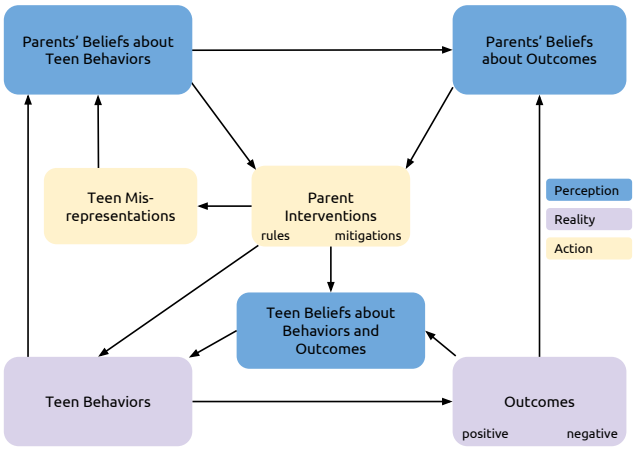


**Figure 1. An influence diagram showcasing the relationships between teens' behaviors and the outcomes of those behaviors.**

teens, termed *teen misrepresentations*, whereby teens try to circumvent parents' rules or mitigation strategies.

Both teens' behavior and parents' interventions can be affected by their own perceptions of what behavior teens are engaging in and by their perceptions of the positive and negative outcomes of those behaviors. Parents' beliefs cannot directly change a teen's behavior without the parent first employing some intervention strategy. The intervention may be the parent communicating their beliefs to the child, but the intervention is a necessary intermediary.

## RESULTS

We begin with some discussion of teens' online behavior and the outcomes of that behavior. We move on to discuss parental interventions in-depth, and demonstrate major points of both agreement and disagreement among our experts. We conclude with discussion of the ways teens misrepresent their online activities to avoid these interventions.

### Teens' Online Behavior and Outcomes

Our experts reported that teens are doing everything online, but especially chatting. As R3 put it, "Most kids just want to talk to people they know."

The way teens connected with their friends, however, was often foreign to the experts. I1 explained, "[teens] can be sharing selfies right with someone who's standing ten feet away." R1 described the same behavior less charitably: "they feel that they have to take pictures to share with everybody without enjoying their surroundings." Similarly, experts in the child protection software industry felt that teens didn't spend enough time offline. P1 derided online games: "physical activity, you know, like going and playing an actual game versus playing on online game," and P2 stated that studies say teens are online for 10 hours a day.

Many of the negative attitudes towards engaging online expressed by our participants could be attributed to the shifting of social and personal norms since the rise of digital media—a generational disconnect. One such example was password, device, and account sharing, which was observed by a few of our experts. In the words of R1: "They love to share passwords and access one another's social networking." R3 believed that this was a show of trust, especially between teen girls. But sharing access to one's online accounts with another person is a clearly risky activity. L1, a cybercrime investigator, cautioned that if a teen shared their password with another person, that person might "say or do something that's not appropriate" under the teen's name.

In this vein, we asked experts about negative outcomes that teens face as a result of their online activity. The experts mentioned many topics, including opportunity costs to schoolwork and sleep, loss of privacy, and long-term embarrassment as a result of digital records. However, we focus here on the two risks that most captured our experts' attention: communicating with strangers online and cyberbullying.

| Intervention | Examples |
|---|---|
| Software Monitoring | Using parental controls and other software tools to monitor what teens are doing online. |
| Nontechnical Monitoring | Looking at teens' social media accounts and reading their posts and messages to monitor what teens are doing online. |
| Rules and Guidelines | Time limits on device use, taking away devices as punishment, telling not to share certain content |
| Fear Appeal | Telling teens about how other teenagers' unsafe online actions have had serious consequences for their personal safety to warn against those actions. |
| Education | Teaching teens about what online activity they consider appropriate, and how to handle potentially unsafe situations online. |
| Communication | Discussing online activity and unsafe situations with teens, including back-and-forth questions and sharing experiences. |
| Parental Complacency | Letting teens experience social media on their own, without interjecting additional information or oversight. |

**Table 2. Examples of the parental intervention methods we discuss.**

*Stranger Danger*

One of the most-discussed risks of teens' online activities is that they might talk to strangers and be abused as a result. Our participants who were most concerned with this risk considered it an inevitable eventuality of unmonitored Internet use. LR1 relayed a story exemplifying this belief:

> I had someone who told me he got a six-year-old an iPhone, and the other children all have iPhones too, and he was like, "they are all linked so I know what is happening." And I was like, "well, I beg to differ," and then it turned out... there was a predator talking to his kids.

L1, also a cybercrime investigator, admitted, "I cannot think of anything good" about talking to strangers online when pressed, and though L2 felt that "taking an online relationship with a stranger offline is not as commonplace," she was concerned about "creepy" strangers "just sort of sitting and watching what [teens are] doing online."

For some, the danger was less specifically abuse and more generally, as R5 put it, "the riskiest thing is that you can't always know who is on the other end." These experts were concerned that online-only communication made it difficult for children to determine which strangers were most risky. Educator E1 lamented, "I wish that there was a way that a software tool could actually cross-check or legitimize a person's age."

On the other hand, some experts felt that the risk of online stranger danger was overblown. E2, an author who lectured about cybersecurity in schools, called the most dangerous cases "rare instances." R2 stated that media reports about online strangers "lead people to worry about and be cautious about things that aren't really particularly dangerous and distract them from things that are dangerous."

R3 stated that despite popular focus on stranger danger, in her experience, most teens were resilient to online advances from strangers. She explained she worries about "the same kids that I worry about on the playground." Researcher R4 further stressed resilience, cautioning that if teens are too sheltered from interacting with strangers, "when they do encounter a risky situation they might not learn how to deal with it."

A few of our experts discussed benefits of talking with strangers online. I1 discussed the impact that online acceptance can have for "kids who are trying to figure out their sexual identity" who feel unsafe in their offline community. R5 relayed an anecdote about her daughter receiving a comment on Instagram from a musician, which "inspired [her daughter] to not only continue being a fan of that band, but to get more interested in different kinds of music."

*Online Bullying*

Most of our participants, especially the educators, had observed cyberbullying among teens. E1 described students trolling and starting rumors online, and E3 observed students passing around videos to laugh at their subject. Our experts largely felt that this behavior was not prompted by the internet. In E2's words, echoing R3's statements about stranger danger above, "the risks are not all that different than if they were on the playground or in the library or whatever... It's just that the potential audience is so much greater."

With a larger audience come new concerns. Industry technologist I2 worried about the "risk of a lack of context," cautioning that comments between friends could be interpreted negatively. And P2 noted that whatever happens online could be "disseminated in a much more accelerated public way," exposing victims of bullying to even more negative attention.

Parents may not be equipped to handle the spread of bullying through online platforms. As R3 and R4 both noted, the media tells stories of cyberbullying that has resulted in extreme consequences, artificially inflating the perceived likelihood of those outcomes. Parental anxiety might be further worsened by how broadly adults define bullying.

R6 stated that although teens tended to have a very narrow view of bullying, adults defined it much more expansively: "every form of meanness and cruelty to light weight teasing and taunting, to serious forms of egregious victimization that would normally be criminal harassment." R3 further reinforces this, saying that adults respond to "a real range of behaviors... some of which are absolutely ridiculous because they are not harmful at all."

### Parent Interventions

Our experts talked extensively about the ways that parents intervene to influence their children's behaviors. The experts also expressed how effective they felt these intervention methods were for the average family—these comments may not apply to different family situations, including strained parent-teen relationships. The five most prominent methods are discussed below: software monitoring methods, nontechnical monitoring methods, rules and guidelines, fear appeal, education, and communication. Experts also discussed a common barrier to instituting interventions: parental complacency. These are shown in Table 2.

#### *Software Monitoring Methods*

Our participants were divided on the use of parental controls and other software tools. Four participants (L1, LR1, P1, P2), who were all either cybercrime investigators or child protection software industry members, supported their use in most or all families. The remaining participants either did not support the use of tools or supported only limited use of them.

The pro-monitoring experts' views are characterized by two central tenets. First, a parent must use a monitoring tool to be engaged with their children's safety. P2 explained that without "parenting a child's mobile activity... you'll not really be parenting. Because... it's not a *section* of their life. It's a hugely integrated part of their life." Second, he said, a "[digital] device is a privilege," and a parent who says, "I want to be able to monitor it," is fully within their rights to do so.

From his perspective as an investigator, L1 heavily underscored the view that the use of monitoring software was necessary for modern parents: "some families do have some decent rules where mom and dad put monitoring softwares on their devices. I love those parents. That's awesome. That's one less likely victim I'd have to ever deal with because mom and dad are being proactive and then making rules."

Their endorsement of monitoring software is not surprising, given that these experts expressed more frequent run-ins with seriously harmed teens. L1 spoke frankly about this: "maybe I'm fried from doing what I do... I see too many bad things. I never see really good things." From their perspective, not making use of software tools is not using all available resources to keep teens safe online.

Although the pro-monitoring experts agreed that software is necessary, they did not agree on if parents should be open with their children about using it. P1, who founded a child protection software company, argued not only for kids to be aware, but also for them to benefit: "the child should equally find it useful and cool to use and understand why it is there, just like a parent does." But LR1 felt strongly the opposite: "I think key loggers are great tools for parents to monitor what's occurring. But that being said, I would tell them not to tell the kids because if the kids know they are going to figure out a work around."

The remaining participants all voiced more skepticism towards the use of parental control software. R1 cited considerations for the age and maturity of the child, stating "you cannot have parental control with a 17 year old," and suggested instead of monitoring, software should provide teens with "tips and awareness before they click on anything." L2 was okay with parental controls for "really little kids," but was uncomfortable with the use on most children. E2, who lectures to both teens and adults about cybersecurity, staunchly opposed the secretive use of software, saying, "I think it teaches a bad lesson to kids about trust and about honesty." R4 suggested that tools could analyze those activities automatically and then help teens "be aware of their own behavior."

Other experts had even stronger reactions to the use of monitoring software. R5 called it "egregious," and R3 stated, "we've put a lot of paranoid action into parental controls that are highly invasive." R3 further argued that the use of software by an adult "makes it harder for [teens] to go to that adult if they actually need help," echoing E2's sentiments about software and trust. R6 felt that teens need something software could not provide: "you need to find a loving adult in their world... Technology, for me, doesn't do it without having the people on the other end."

Finally, R2 regarded the use of software as a distraction: "I think the idea of catching kids doing things has limited utility, because generally what you're doing is catching kids after the fact when what you really want to be doing is preventing these kind of problems."

#### *Nontechnical Monitoring Methods*

Opinions on the use of nontechnical monitoring methods were similarly divided between the pro-monitoring experts and the others, though more experts outside of the pro-monitoring segment fell into a middle ground.

Some experts felt that a parent should look at teens' online accounts, read their messages, and generally keep tabs on what teens were up to by having access to and reading about their activity. L1 endorsed a concept he called verification, whereby parents should actively check teen's accounts for signs of unsafe behavior: "I don't want to just take [their] word on it. I want to see it." LR1 affirmed this, saying, "parents have a right to check every device."

Though the staunchest supporters of monitoring held firm for both software-assisted and nontechnical methods, many experts who expressed distaste for monitoring software were open to nontechnical monitoring. Attorney E2 advised that, "until [teens are] legally responsible for [themselves], that right to privacy is conditional on [their] behavior." I1, who works on online safety policies for industry, similarly relied on age, describing a maturation process for parent oversight: "you'll go from the total parental, like, dos and don'ts to a place where you're having conversations, to a place where eventually you're two adults who are interacting."

One expert described parents' struggle over monitoring with a personal anecdote. R5 admitted that "if I picked up my daughter's phone right now there would be things that would shock me and not make me very happy." But she restrained herself from taking this step, realizing that her own fears, not her daughter's actions, materialized the desire to read her daughter's correspondence.

Another expert, educator E1, discussed how to reframe monitoring practices as a learning experience for both parent and child. She suggested a parent have the teen "sit right next to them" as the teen explained what they were doing online so that the parent has a chance to express concerns and ask questions, and the teen has a chance to educate the parent about how to use social media.

These nontechnical practices have detractors. R1 lamented the "feeling that you have to monitor your teen 24/7 online," and R3 channeled a concerned parent: "I guess I have to spy on my kids because I'm told that's the only way I can keep them safe." Researcher R4 likewise protested how a "reactionary" parental response to unsafe online behavior "becomes [more] of a privacy violation for that teen."

#### *Rules and Guidelines*

Our experts liked rules that limit online use: "I think rules like banning devices at the dinner table, during family dinner are very important," stated R2, a bullying researcher. Cybercrime investigator L1 cited bedtime limits that even parents obey, which show, "We don't need it. You don't need it," and encourage teens to use devices in moderation.

The experts offered ideas for making these rules work: R1 suggested engaging teens in the process, "because they consider themselves to be part of the decision-making." E1 and I1 favored a mutual agreement between parent and child: "here are the parameters that we're gonna set up for use. You agree to this and I agree to that." I1 further believed that expectations should be set "before the child gets onto social media." R4 explained that younger teens needed rules "because they're more novices about going online."

Expert E1, in her role as an educator, shared a guideline she used to encourage kids to reconsider what content they were sharing online:

> I say to them, "Imagine if you were doing this on a computer. The images from your phone can be emailed." And I always tell the kids, "Imagine if that email was put on a smart board or projector," and they're like, "Whoa... I wouldn't send a picture of myself if I knew it was going to be projected onto this huge screen."

However, experts felt rules often lacked the consistency to make them fully effective or were not realistic for teens. LR1, formerly in law enforcement, was wary of rule-setting without followup: "parents think if the computer is in the main room... then we're good." She felt that teens could easily slip into risky behaviors when they realized their parent was not watching them. And educator E2 noted that teens might correctly say, "Well, you can't take away my device 'cause I have to do my homework." Making rules about online behavior, E3 says, is "not going to be effective if you're not acknowledging what kids are actually wanting to do."

Notably, most of the rules and guidelines that our experts addressed were aimed at physical devices, preventing loss of sleep, and encouraging more offline social time. But our participants largely did not tackle rules about online privacy and security for teens, which would encourage healthy engagement with the Internet and not just digital devices.

#### *Fear Appeal*

Many of our experts cautioned against the use of fear appeal. R2 expressed particular opposition: "generally speaking, trying to frighten people into doing the right thing is usually less effective than talking to them, and realizing that not everyone engages in high-risk activities."

However, a few participants strongly supported using the fear appeal. Law enforcement professional L1 declared, "it's not a scare factor. It's a truth factor." And P1 described the "pale faces" and "freak[ed] out" reactions to his online safety presentations as positive proof of their effectiveness. Nonetheless, he later warned about the dangers of "kneejerk reactions" to "fearmongering." Similarly, LR1 described how teens react poorly to parents' attempts to scare kids, but continued, "I give presentations and I always scare kids, always, and they always tend to believe me and trust me... because I'm an outside third party."

#### *Education*

Most of our experts mentioned the importance of education about appropriate online behavior during their interviews—but the focus was on parents. Researcher R4 described parents as having a "naïve hope that teens are learning online safety at their school."

The experts promoted educating parents, so that parents could, in turn, educate their children. LR1 urged parents that, "keeping up with technology and the trends is very, very important and helpful." Educator E1 described how she demonstrated privacy controls to parents: "with an iPhone when [teens are] using location services, letting parents know that you can turn this off, this is how to turn it off."

The experts proposed many different ways of educating children. E2 espoused modeling behaviors, saying, "be a good digital role model. That is, don't do things yourselves that you don't want your kids doing." L2 suggested that parents pair education with rules-setting. She stated that "there has to be more of an explanation as to why things happen the way they happen," such as why it is dangerous to talk to strangers.

Other education methods rely on teens learning through firsthand experience and peer knowledge. R4 stated that facing and overcoming small risks provided "learning opportunities" for dealing with larger ones. R1 supported peer learning: "the best things for teens is to engage them and let them disseminate that information among one another."

Experts agreed that when educating children, parents should start early. In I2's words: "Don't wait 'til your teen is a teen... If you haven't built that ethical foundation from the time that they're seven and up or even younger, don't expect them to let you in." Parent-guided engagement with the internet from a young age may give children the foundation needed to build a healthy relationship with online spaces.

#### *Communication*

Regardless of how our experts valued other parental interventions, they all felt that parents needed to communicate with

teens. As P2 said, "part of being a parent is a deep relationship with your child." Unlike education, communication relies on a dialogue between parent and child: parents need to ask teens questions and allow teens to "openly explore the questions that they have," as educator E3 states.

These conversations aren't always easy for teenagers, so R3 advises "daily contact where [parents and teens] just chitchat, not quality time, because that doesn't exist, just lots of quantity time so they can come and bring something up whenever they need to," and R6 additionally suggests that parents encourage relationships between teens and "adults who are not immediate authorities that are part of their communities." This contact, E1 says, lets teens know "if they have a concern that an adult will take it seriously."

Teens need conversation to "process what's happening," suggests expert R4. LR1, a former law enforcement professional, is afraid that parents don't "talk about the bad things that happen online." R5 notes: "When you see your child doing something that shocks you, and upsets you... that's an opportunity to have a conversation."

#### *Parental Complacency*

Experts were united in warning against parental complacency as a result of being unaware of teens' online activities or current technology. P2 described the dilemma of when to intervene: "It's very hard for a parent to know when is appropriate and when isn't." L1 elaborated, "Mom and dad, in today's world, both work jobs. Everyone's working. There's no time. There's no attention." R5 also warned, "we have got parents who are overwhelmed by the technology, unaware of what the risks are, or you know just—I don't want to say ignorant, because that seems harsh—naïve to the risks."

All experts felt that these inactive parents didn't take "part of the ownership," as R5 stated, for their children's online behavior. E3 emphasized that some parents are "not taking a stand" about appropriate online behavior. She urges that adults should provide guidance when actions are not safe.

When parents are unsure about technologies, and feel that they can't make decisions, our experts said: your teens can be a resource. E1 mimed a naïve parent's thought process, concluding with a call for action:

> "I don't know what I'm doing. [My kids] know what they're doing. I'm just going to step back and let them do what they're doing." Completely ineffective. Let them teach you. Let them show you how.

### Teen Misrepresentations

Teens are getting around parental interventions in numerous ways, but most of our experts say they're opting to fake out the parents. P1 states they could be "using [a] friend's device to connect," which would avoid both software-enforced monitoring and nontechnical monitoring. E1 says teens "create their account with a different name," so parents cannot tell what to monitor or verify if their rules are being followed.

Further complicating digital monitoring, LR1 says teens use "messaging apps, where the parent can't necessarily get that data" without physical access to the device. E2 adds, "there are actually apps that you can buy which allow you to change the icons and the names of apps that you use so that they really look innocuous," which might thwart a parent's attempt to monitor teens' behavior by physically accessing the device.

The creativity of teens' evasion methods doesn't end there. R6 described how teens would use the comments section of personal blogs of young adult novelists—which were accessible on heavily filtered school computers—to have conversations in plain sight while in school computer labs.

With so many ways for teens to evade parents' mitigation strategies, we are faced with the question of what interventions parents should be trying for the best chances of success. R2 writes off monitoring software, saying it's "not really difficult to get around technological approaches." On the opposite side of the fence, P2 advocates hiding the use of monitoring software in extreme cases: "If the child knew that the parent was doing this, the child would either rebel, find another way to communicate and hide their risky behavior... and so and it would fracture the relationship with the parent and these relationships can be very tenuous."

But one expert argued that sometimes, teen pushback against monitoring could be positive. L2 said, of teens blocking their parents online, "I think it's actually good for the kids to learn how to draw boundaries and sort of create spaces for themselves." She was opposed to parents forcing their children to unblock them, citing the boundary as a sign of growth.

Though teens misrepresenting their online behavior to their parents or other adults can be risky, the prevalence of this topic signals that some amount of evasion must be normal. A software tool that encourages conversation between parents and teens about online behavior, and encourages teens to share with their parents, start discussions, or ask questions, might go a long way towards easing parental fears without the privacy concerns of traditional monitoring software.

## DISCUSSION

Our results suggest a tension between safety and privacy. We offer novel technological approaches which could allow parents to intervene in a way that promotes both.

### Expert Dichotomy

We found that our experts fell into two groups, based on whether they viewed the use of software monitoring risk-mitigation methods by parents as necessary. The experts who worked in monitoring software companies or cybercrime investigation tended to advocate for these methods. Among the other experts interviewed, monitoring software or requiring access to a teen's accounts were either viewed as ineffective, too privacy-invasive, or appropriate only for younger children.

The values of both groups of experts likely originate with their experiences. For pro-monitoring experts, strict security measures are the only solution that makes sense given that they have seen so many grievous harms. In contrast, the experts who supported only moderate monitoring practices saw a more diverse range of outcomes, which led them to suggest a more diverse set of parenting practices suited to individual families.

All participants mentioned the value of parent-teen communication about teens' online behavior. They agreed that discussions were more likely to result in teens respecting and understanding parenting decisions. The experts who did not advocate for monitoring methods did suggest parents use rules, education, and communication to reduce risky behavior.

Many of our experts discussed positive outcomes of teens' online behavior. As today's teens mature, they rely on digital environments to explore friendships and identity, seek acceptance, educate themselves, and find opportunities. Some experts mentioned that very privacy-invasive monitoring would make this healthy exploration difficult for teens. Experts who stated they did not believe teens had privacy rights from their parents did not discuss these benefits.

In cases where teens are involved in high-risk behaviors, monitoring action may be necessary. These teens would likely benefit from more intervention and specialized mitigation efforts. However, many of our expert participants feel these situations are not common, and say that most teens should not be strictly monitored. This suggests that parent interventions can vary depending on each family, and each child within that family, based on individuals' needs.

### Digital Interventions

Whereas some of our participants weighed safety over privacy, others suggest the opposite. We believe that parents' mitigation strategies should be less of a tradeoff between privacy and safety. We discuss eight ideas for digital interventions, motivated by needs identified by our experts.

Our experts noted that teens were sharing passwords and access to devices with their friends. By doing so, teens are exposing themselves to security and bullying risks. Warning teens off of this would probably not be successful, as the sharing serves a social purpose. We should be asking what teens want their friends to have access to when they decide to share passwords. We could envision a service that gives a friend access to some messages without access to the account.

Our experts also wished for a technical solution that could clearly indicate when a contact request was sent by a stranger. Key factors that define a stranger were identified by our experts, including the person's age, location relative to one's own, mutual friend network, and record of activity, or lack thereof, on the website or app. Intercepting contact between teens and strangers with a warning before the teen gets to know and trust the stranger could prevent harms in cases where the teen did not intend to talk to an unknown adult.

When teens intend to talk to strangers, an intervention might help them determine how trustworthy the strangers are. This could aid teens looking for communities to explore their identities so that they find welcoming, safe places. This could also help teens to learn the resilience mentioned by R4, as teens see explanations of why this stranger might be risky.

Some experts suggested that parents and teens sit down together and go through the teen's social media presence as an educational experience for both parties. A social media platform could provide a tutorial that they complete together, which might include discussion prompts about adding friends and who can see the child's posts.

All of our experts expressed that parents should actively discuss online activity with their teens outside of the context of specific applications. A software tool might prompt parents with conversation topics or educational articles to keep them actively engaged with their child about appropriate online behavior, helping to fight parental inactivity.

Another tool for parents and teens might allow the teen to reach out to parents when they see upsetting content. The teen could forward content to the parent along with a message, facilitating a discussion how the teen might handle the situation it presents. This would also allow teens to share instances of online conflict and express their views first, without an adult jumping to label it cyberbullying. This might enable adults to provide support and guidance without the teen disengaging.

Another expert view was that monitoring intensity should decrease as a child becomes older and more mature. Monitoring software might include an option to "back off" of detailed monitoring automatically as the child gets older and demonstrates continuously safe behavior. The parent would get gradually less explicit records of the child's activity, but the software could still watch out for warning signs of risky behavior and jump in to alert the parent as needed.

Experts also suggested that teens would benefit from warnings at the time of risky behavior. A tool could prompt teens to reconsider their actions, such as with questions like, "Are you sure you want to post that publicly?" or "Do you really know this person you are about to friend?"

Finally, any number of these tools could base their underlying technology on machine learning to identify risky behavior. A detection system might adapt to an individual teen's pattern of behavior to more accurately identify when they are engaged in risky activities. Research with teens and parents to examine their actual beliefs, behaviors, and communication would be useful to guide the development of these tools.

## CONCLUSION

We interviewed 16 experts about teens' online behavior, the outcomes of that behavior, and parents' mitigation methods. We found that experts are most divided over the effectiveness of different mitigation strategies. Our experts agreed that communication, education, and rules are useful tools for parents to mitigate risky teen online behavior. Experts who frequently encountered very negative outcomes were more supportive of monitoring and fear appeals, whereas others encouraged use of those techniques in moderation, or discouraged them completely. As a result of our findings, we suggest tools that address negative outcomes, encourage mitigation methods that all of our experts supported, and discourage unnecessary privacy invasion.

## REFERENCES

1. Tawfiq Ammari, Meredith Ringel Morris, and Sarita Yardi Schoenebeck. 2014. Accessing social support and overcoming judgment on social media among parents of children with special needs. *Proc. ICWSM* (2014).

2. 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*. ACM, 3895–3905.

3. danah boyd. 2014. *It's Complicated: the social lives of networked teens*. Yale University Press.

4. Amy Bruckman, Kurt Luther, and Casey Fiesler. 2015. When Should We Use Real Names in Published Accounts of Internet Research? *Digital Research Confidential: The Secrets of Studying Behavior Online* (2015), 243.

5. Lorrie Faith Cranor, Adam L Durity, Abigail Marsh, and Blase Ur. 2014. Parents' and teens' perspectives on privacy in a technology-filled world. In *Proc. SOUPS*.

6. Julie S Downs. 2014. Prescriptive scientific narratives for communicating usable science. *Proceedings of the National Academy of Sciences* 111, Supplement 4 (2014), 13627–13633.

7. Julie S Downs, Mandy Holbrook, and Lorrie Faith Cranor. 2007. Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*. ACM, 37–44.

8. Julie S Downs, Mandy B Holbrook, and Lorrie Faith Cranor. 2006. Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security*. ACM, 79–90.

9. Elizabeth Englander. 2012. Low risk associated with most teenage sexting: A study of 617 18-year-olds. *MARC Research Reports* (2012).

10. Skyler T Hawk, Loes Keijsers, William W Hale III, and Wim Meeus. 2009. Mind your own business! Longitudinal relations between perceived privacy invasion and adolescent-parent conflict. *Journal of Family Psychology* 23, 4 (2009), 511.

11. 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*. ACM, 583–599.

12. Amanda Lenhart, Maeve Duggan, Andrew Perrin, Renee Stepler, Harrison Rainie, and Kim Parker. 2015. Teens, social media & technology overview 2015. http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/. (April 2015).

13. Sonia Livingstone and Magdalena Bober. 2006. Regulating the internet at home: Contrasting the perspectives of children and parents. *Digital generations: Children, young people, and new media* (2006), 93–113.

14. Mary Madden, Amanda Lenhart, Sandra Cortesi, Urs Gasser, Maeve Duggan, Aaron Smith, and Meredith Beaton. 2013. Teens, social media, and privacy. *Pew Research Center* 21 (2013).

15. Alice Marwick and danah boyd. 2014a. 'It's just drama': teen perspectives on conflict and aggression in a networked era. *Journal of Youth Studies* 17, 9 (2014), 1187–1204.

16. Alice E Marwick and danah boyd. 2014b. Networked privacy: How teenagers negotiate context in social media. *new media & society* (2014), 1461444814543995.

17. Alice E Marwick, Diego Murgia Diaz, and John Palfrey. 2010. Youth, privacy and reputation. *Harvard Law School Public Law & Legal Theory Working Paper Series* (2010), 10–29.

18. Aaron Metzger, Christa Ice, and Lesley Cottrell. 2012. But I trust my teen: Parents' attitudes and response to a parental monitoring intervention. *AIDS research and treatment* 2012 (2012).

19. Anca Micheti, Jacquelyn Burkell, and Valerie Steeves. 2010. Fixing broken doors: Strategies for drafting privacy policies young people can understand. *Bulletin of Science, Technology & Society* 30, 2 (2010), 130–143.

20. Tehila Minkus, Kelvin Liu, and Keith W Ross. 2015. Children Seen But Not Heard: When Parents Compromise Children's Online Privacy. In *Proceedings of the 24th International Conference on World Wide Web*. International World Wide Web Conferences Steering Committee, 776–786.

21. Margaret K Nelson. 2010. *Parenting out of control: Anxious parents in uncertain times*. NYU Press.

22. Gjalt-Jorn Ygram Peters, Robert AC Ruiter, and Gerjo Kok. 2013. Threatening communication: a critical re-analysis and a revised meta-analytic test of fear appeal theory. *Health Psychology Review* 7, sup1 (2013), S8–S31.

23. Sandra Petronio. 1994. Privacy binds in family interactions: The case of parental privacy invasion. In *The dark side of interpersonal communication*, W. R. Cupach and B. H. Spitzberg (Eds.). Lawrence Erlbaum Associates, Inc, Hillsdale, NJ.

24. Priscilla M Regan and Valerie Steeves. 2010. Kids r us: online social networking and the potential for empowerment. *Surveillance & Society* 8, 2 (2010), 151–165.

25. Nancy Jo Sales. 2015. Tinder and the Dawn of the "Dating Apocalypse". *Vanity Fair* (September 2015).

26. Sarita Yardi Schoenebeck. 2013. The Secret Life of Online Moms: Anonymity and Disinhibition on YouBeMom.com.. In *ICWSM*.

27. Maanvi Singh. 2015. Less Sleep, More Time Online Raise Risk For Teen Depression. http://www.npr.org/sections/health-shots/2014/02/06/272441146/less-sleep-more-time-online-amp-up-teen-depression-risk. (February 2015).

28. Judith G Smetana. 2008. “It’s 10 o’clock: Do you know where your children are?” Recent advances in understanding parental monitoring and adolescents’ information management. *Child Development Perspectives* 2, 1 (2008), 19–25.

29. Amos Tversky and Daniel Kahneman. 1974. Judgment under uncertainty: Heuristics and biases. *science* 185, 4157 (1974), 1124–1131.

30. Pamela Wisniewski, Haiyan Jia, Na Wang, Saijing Zheng, Heng Xu, Mary Beth Rosson, and John M Carroll. 2015a. Resilience Mitigates the Negative Effects of Adolescent Internet Addiction and Online Risk Exposure. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 4029–4038.

31. Pamela Wisniewski, Haiyan Jia, Heng Xu, Mary Beth Rosson, and John M Carroll. 2015b. Preventative vs. Reactive: How Parental Mediation Influences Teens’ Social Media Privacy Behaviors. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*. ACM, 302–316.

32. 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*. ACM, 3919–3930.

33. Pamela J Wisniewski, Heng Xu, Mary Beth Rosson, and John M Carroll. 2014. Adolescent online safety: the moral of the story. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*. ACM, 1258–1271.

34. Kim Witte. 1998. Fear as motivator, fear as inhibitor: Using the extended parallel process model to explain fear appeal successes and failures. (1998).

35. Sarita Yardi and Amy Bruckman. 2011. Social and technical challenges in parenting teens’ social media use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 3237–3246.