An Examination of Parenting Strategies for Children's Online Safety

Abigail Marsh

CMU-ISR-18-106
August 2018

Institute for Software Research
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

Thesis Committee
Lorrie Faith Cranor, Advisor
Julie S. Downs
James D. Herbsleb
Amy S. Bruckman, Georgia Tech

Submitted in partial fulfillment of the requirements for the
degree of Doctor of Philosophy in Societal Computing

©2018 Abigail Marsh

Abstract

Teenagers are using the internet for a variety of social and identity-based activities, but in doing so, they are exposed to risky situations. The work of ensuring teens' online safety largely falls to parents, many of whom are unprepared to understand the realities and norms of teens' online activity. In this thesis, we investigate how parents and teens perceive online risks, the effects of using current tools designed to keep teens safe online, and finally, the usability of currently available online safety tools. We have conducted interviews with parents and teens to understand how they perceive digital privacy within their families, and in what situations teens' privacy should be preserved or denied. We investigated a specific case of online safety, peer-based online conflict among teenagers, also called cyberbullying. We studied whether and how parents and teens define cyberbullying and a related concept, "drama," differently. We explore the pressures parents face to employ privacy-invasive and restrictive parenting practices, and their confusion about teens' digital communities that make some parents unsure about communication and education-based interventions. We identified a set of seven parenting strategies through interviews with online safety professionals. We explored these strategies through a longitudinal study of parenting software and behavior contracts in comparison to a control condition. Specifically, we measured the impact of one month of using these tools on participants' perception of online risks and the usability challenges of these tools. Overall, this thesis highlights the importance of developing usable online safety tools built for both parents and children as primary users.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Teenagers are using the internet for a variety of social and identity-based activities, but in doing so, they are exposed to risky situations. The work of ensuring teens' online safety largely falls to parents, many of whom are unprepared to understand the realities and norms of teens' online activity. This thesis investigates how we can improve family online safety interventions in ways that both encourage teens to avoid risky online behavior and provide less privacy-invasive tools for parents to ensure their child's safety. We studied how two parenting interventions, a parental control software and a behavior contract, influenced online risk perceptions in families and the usability challenges posed by those tools in furtherance of this goal.

Adolescence is a period wherein teenagers begin to explore their sense of self, and much of this identity construction is happening online for modern teens [16]. Parents are the first defenders of their children's online safety, but they are often unsure how to guarantee that well-being [29]. There are many online sources, such as monitoring software providers [119] and journalists [47, 55, 118, 129], that encourage online safety practices such as monitoring teens' online behavior or significantly restricting allowed behavior. But research shows that these parenting practices lead to distrust and lessened communication from teens, and can result in teens hiding their behavior from their parents [71, 83, 91, 140].

Existing digital parenting tools frequently encourage parents to prioritize teens' online safety over teen privacy. A paper by Wisniewski et al. analyzed the features of 75 Android mobile apps designed to help teens stay safe online. The authors found that those apps were targeted at parents for monitoring or restricting teens' behavior; considerably fewer apps offered any self-regulation features for teens, and those that did relied heavily on options for the teen to reach out for help from an adult [130].

Some parents might choose instead to avoid tension between themselves and their children by allowing the child to have unmonitored, unrestricted access to the internet. Children of current generations have been called "digital natives," and they are assumed to be able to navigate the risks of interacting with other people online fine on their own [100]. However, other researchers dispute the idea the "digital native" generation is naturally able to handle online risks without ever receiving adult guidance [14]. Further, boyd has reported that the skill sets needed to navigate online risks may be unequally distributed across demographic factors and individual access to digital devices [16], indicating that simply growing up in an age of ubiquitous computing is not enough for children to learn how to avoid risky situations online.

Parents concerned with their childrens' online safety are choosing from a set of options that are often frustrating and unfulfilling for both parent and child. However, experts suggest that parenting a child's online behavior does not need to be these things. In interviews with experts, we

have found support for monitoring practices, which experts say encourage parents to be attentive to their children [78]. Experts in this study also suggest that parents communicate with their children about online safety to encourage mutual respect and create an open dialog [78]. In this work, we examine parenting strategies to understand how they can be improved for the benefit of both parents and children.

In Chapter 2, we investigate parent-teen privacy decision making through semi-structured interviews with 10 teenagers and 10 parents of teenagers. Parents and teens generally agreed that teens had a need for some degree of privacy from their parents and that respecting teens' privacy demonstrated trust and fostered independence. We explored the boundaries of teen privacy in both the physical and digital worlds. Though parents commonly felt none of their children's possessions should ethically be exempt from parental monitoring, teens felt strongly that cell phones, particularly text messages, were private. Parents discussed struggling to keep up with new technologies and to understand teens' technology-mediated socializing. While most parents said they thought similarly about privacy in the physical and digital worlds, half of teens said they thought about these concepts differently. We present cases where parents made privacy decisions using false analogies with the physical world or outdated assumptions. We also highlight directions for more usable digital parenting tools.

In Chapter 3, we interviewed 16 experts in fields related to teens' online safety, and surveyed 469 parents ($n = 244$) and teens ($n = 225$) about their perceptions of the effectiveness and acceptability to teens of different parenting strategies. From the interviews, we established seven categories of strategies, of which our experts had mixed opinions. Some categories, like educating teens, were supported by all; others, like monitoring children using software, inspired strong feelings for and against. From our surveys, we found that though parents and teens rated some strategies similarly, their rankings of parental inaction and monitoring speak to how teens and parents value those teens' privacy versus safety differently. Our results highlight distinctions among parenting strategies that have been broadly categorized in previous literature, and support the need to study parental complacency alongside active parenting practices.

In Chapter 4, we introduce two longitudinal studies of parenting interventions in practice. We conducted an interview study with 31 pairs of parents and teens and a survey study, data collection ongoing, with additional families. Families were randomly assigned to one of three conditions: use a parenting software for one month, use a behavior contract for one month, or the control condition. We discuss the methods used for these studies, including our recruitment practices, participant demographics, study materials, and analytical methods. We also preview the remaining three results chapters which discuss three distinct focuses of our analyses.

In Chapter 5, we discuss cyberbullying and a related concept, "drama." Experts and families studied in Chapter 3 mentioned cyberbullying as a concern, and we investigated how parents and their children defined cyberbullying. We also probed "drama," an idea introduced by Allen [6] and further expanded by Marwick and boyd [79], which they understood as a teenage construct to compartmentalize certain types of online interactions from the more severe cyberbullying. Participants responded to scenarios that could be classified as cyberbullying or drama and were also asked to define the two concepts. We found that parents and teens largely did not understand drama and cyberbullying differently from each other. They did draw distinctions between drama and cyberbullying, suggesting that the two are separate types of interactions. We highlight an emerging concept, technology-mediated power imbalances, which may be an important facet of cyberbullying.

In Chapter 6, we investigate families' perceptions of online risk and how those perceptions may change with the introduction of parenting tools. We asked participants in our longitudinal studies to respond to a series of likert questions about various online safety risks. Each risk was evaluated

for its severity, likelihood, the parent's ability to protect their child from the risk, and the child's ability to protect themselves from the risk. We did not find a robust change in risk perception from using either of the parenting tools, likely due to the small sample size of our studies. We expect that if either of these tools had a large effect on how parents or children evaluated risks, that would be visible in our sample. We did find that parents rated their ability to prevent online risks from happening to their children significantly lower than children's ratings of the same. This suggests that children may substantially rely on their parents to make sure they aren't engaging in risky behavior but that at the same time, parents are not sure they have adequately protected their children. We highlight the importance of tailoring risk interventions so that the severity and likelihood of a risk event happening are commensurate with the impositions of the intervention on both the parent and child.

In Chapter 7, we discuss the usability of the two parenting tools we tested in our longitudinal studies. The first was a parental control software, Qustodio, and the second was an online behavior contract, The Smart Talk. We observed families set up both the software and the contract in our lab. Our observations and the families' conversations form the basis for this analysis. We found that both tools posed usability issues. The contract handled setting device use time limits particularly poorly, and this was often a point of contention within families. The software caused confusion throughout its settings interface because features were not explained and important notices were visually de-emphasized. These are avoidable usability issues that might have been fixed with user testing.

This thesis contributes a longitudinal examination of parental control software and behavior contracts in real families. This is based on work to categorize different types of parenting strategies and contextualize how they are perceived by parents, children, and professionals. We additionally contribute an evaluation of the usability challenges of these interventions. In parallel, we examine the risky behavior that these parenting strategies aim to prevent. We contribute a current analysis of one of those risks, cyberbullying, and its cousin, drama, which suggests that the concepts are distinct and understood similarly by children and their parents. We also contribute the finding that parents feel much less confident in their ability to protect their children from online risks than do their children. Overall, these contributions paint a picture of families in need of improved parenting interventions that are specifically tailored to the most likely and severe risks and that acknowledge the impact of restrictions on the child and provide a structured system for easier negotiations of rules between parents and children.

Chapter 2

Parents' and Teens' Perspectives on Privacy In a Technology-Filled World

In the last twenty-five years, the daily life of a teenager has changed drastically. When the parents of today's teenagers were themselves teens, they had no smartphones connecting them to resources across the globe in an instant. In fact, except in rare cases, they had no mobile phones at all. Twenty-five years ago, teenagers only had access to the Internet at college or via Prodigy, Compuserve, or AOL. Stanley Milgram was the king of social networks; Mark Zuckerberg was just starting elementary school. Photos were developed in a darkroom or on Polaroid film, not Snapchatted.

While parenting has always been tough, these rapid shifts in technology create additional challenges for today's parents. Teenagers are more likely than their parents to understand popular technologies, services, and devices. They are also likely to socialize with friends using these technology-mediated channels. As a result, parents cannot necessarily draw from their own teenage experiences when making decisions about privacy for their children.

In this chapter[1] , we investigate how parents make decisions about privacy for their teens in a world that is far different than the one in which they came of age. We focus on parents' privacy decision making, as well as both teens' and parents' perspectives on the degree to which teenagers should have privacy from their parents. Through semi-structured interviews, we explored four main research questions about teen privacy:

1. From teens' and parents' perspectives, what are the bounds of teens' right to privacy from their parents?

2. How do parents decide how much privacy teens should have when they use new technologies and services?

3. How do parents use parental controls, monitoring software, and ad-hoc approaches regarding teen privacy?

4. How do parents' approaches to privacy in the digital world compare to those in the physical world?

To investigate these research questions, we conducted semi-structured interviews with ten teenagers and ten parents of teenagers. Interviews covered teen privacy in the familiar physical

---

[1]This chapter is a lightly edited version of a paper published as: L. F. Cranor, A. L. Durity, A. Marsh, and B. Ur. Parents' and teens' perspectives on privacy in a technology-filled world. In *Proc. SOUPS*, 2014.

world (e.g., closed doors and dating), in the technology-mediated digital world (e.g., smartphones and social media), and from a philosophical perspective. We focused our questions and analysis on privacy in the digital world and on parents' decision making process, using privacy in the physical world and on a philosophical level to contextualize attitudes about privacy in the digital world.

We found that most of our parent and teen participants agreed that teens should have privacy from their parents, albeit to a limited extent. This right to privacy derived from factors like trust and the desire to foster independence, but was limited by reasons including parental concern and safety. In the physical world, parents generally gave teens some degree of private space at home and in their social lives, such as by knocking before entering a bedroom.

In contrast to parents, teenagers viewed their cellphones, especially text messages stored on their cell phones, to be particularly private. Eight of the ten teens, versus four of the ten parents, felt it unethical for parents to look through teens' text messages. Teens were far more comfortable with their parents accessing their email accounts or Facebook, both of which they used rarely.

We unpack parents' processes for evaluating and regulating their children's privacy, finding that parents largely struggle to make these decisions. In particular, our parent participants often did not understand teens' use of technologies that did not exist when the parents were themselves teens. While half of the teen participants said they think about privacy in the digital world differently than in the physical world, only two parents distinguished between these scenarios. Even though most parents wanted to give their teens private space, they did not always realize the degree to which teens' private spaces are text messages and apps.

Our results aid in understanding the complex issue of privacy as teenagers transition from dependent children to independent adults. This understanding can inform designers of software tools that directly or indirectly impact teen privacy. We discuss the shortcomings of existing digital parenting tools; we also speculate on directions for designing tools that better remind teenagers of their parents' expectations and help parents navigate the complex process of making decisions about their children's privacy. Further in this thesis, we expand upon perceptions of parenting tools (Chapter 3) and then, starting in Chapter 4, examine avenues for improvement of existing parenting tools.

2.1   Background

Privacy is a complex concept that means different things to different people. Over a century ago, Warren and Brandeis discussed privacy as the "right to be let alone" [126]. In more modern interpretations, Helen Nissenbaum explained privacy through the idea of contextual integrity [93], while Daniel Solove proposed that privacy is best examined as a family of related concepts [115] and that privacy can be both an individual and a societal good [116].

Privacy as a legal right is even more complex. Privacy laws in the United States are sectoral, varying by industry. While several amendments within the U.S. Bill of Rights have been interpreted as providing some baseline privacy protections to United States citizens [117], most U.S. privacy laws are enacted to address specific concerns. The state of privacy protection in practice, however, often differs from the laws on the books [13]. In many cases, individuals can have de facto rights through social norms and beliefs. This difference between legal definitions and practice is particularly relevant to teenagers because teenagers have few legal rights to privacy from their parents. In practice, however, many parents do give teenagers some degree of privacy.

While the scholarship on privacy rights and laws is broad, it tends to focus on intrusions on individuals' privacy by the government or corporations. Far less has been written about privacy between individuals, and more specifically the aspect of privacy examined in this chapter: the

privacy beliefs and expectations between parent and teenager, especially in regards to digital space. Researchers who study teenagers and technology [140, 81, 104] have identified a surprising lack of studies investigating the role privacy plays in parent-teen relationships, and vice versa.

Marwick et al. surveyed the literature on youth and privacy [81]. They note the particular importance of studying teen privacy relative to technology since much of teens' socialization is mediated by technology. They also highlight findings that teens care deeply about privacy, particularly from parents and teachers [81]. Work by boyd discusses the privacy dynamic between teenagers and parents [16]. She found that teenagers are quite concerned about having privacy from their parents and that parents rarely grant teens privacy without teens negotiating for it. She asserts that even well-intentioned parents "often...fail to realize how surveillance is a form of oppression." Whereas teenagers are boyd's primary subjects, we split our investigation equally between parents and teens. Ur et al. [121] interviewed both teens and parents in the more narrow context of home security systems with audit logs. They found that such Internet-connected home technologies have the potential to harm teen privacy while at the same time improving home security.

Researchers have also investigated teen privacy from parents' perspective. In her book on modern parenting, Nelson notes the hypocrisy of some parents in monitoring their teenagers while at the same time stating that they believe teens have a right to privacy [89]. Petronio describes ways in which parents invade their children's privacy, as well as teens' reactions ("children's defensive behaviors") to these invasions of privacy [99]. She notes that parents' and teens' divergent expectations of independence may cause conflict, yet did not explore the gap between parents' and teens' perspectives on teen privacy in any detail. Hawk et al. also found teenagers' perceptions of parental privacy invasion causes conflict, yet the magnitude of conflict differs by family [46]. However, they note that parent-teen conflict sometimes plays a positive role in adjusting parents' expectations.

Synthesizing psychology research, Smetana et al. points out that parents often adjust their parenting styles and attitudes for their different children [113]. Yardi and Bruckman also note that a particular child's maturity is a major factor in parents' decisions [140]. In separate work, Smetana found that parents generally reduce the extent to which they monitor their children as the children progress through adolescence [113].

While some parents monitor their teens closely, other parents prefer not to monitor teens at all [140]. Rode conducted in-home studies of twelve households with children, identifying five major strategies parents use to enforce rules about technology [104]. Some participants actively chose to use software tools to monitor teens' activities, while others preferred to talk with their children about safe behaviors. Metzger et al.explain that parents' differing opinions of teens' right to privacy, as well as the trust in the parent-teen relationship, led the parents they studied to reach different conclusions about the ethics of parental monitoring [85].

Parental monitoring sometimes leads children to share less information with parents. This phenomenon has been documented in traditional disclosure settings, such as conversation [46], but also on social media [48]. Teens' voluntary disclosure of information depends heavily on having a positive relationship with their parents [113]. Livingstone and Bober argue that strict monitoring can "undermine the democratic negotiation of mutual rights, trust and responsibilities between parents and children" [71].

Researchers have also investigated the adoption, as well as the non-adoption, of technologies parents can use to monitor their children. Vasalou et al. conducted a survey of 920 parents to understand why so few parents adopt technologies for tracking their children's location [123]. Many of their participants felt such systems could negatively impact their children's independence, suggesting that parents did feel that children have a right to privacy from their parents. Reaching similar conclusions, Czeskis et al. applied Value Sensitive Design to a series of parental monitoring scenarios, suggesting that context be taken into account when parents are deciding whether or not

to monitor their teens [31]. Based on their analysis, they suggested that teens could have privacy from their parents except in the case of emergency.

In recent years, social media sites have become a battleground for teenagers' privacy from their parents. Although 80% of parents who used social media had friended their teenager on a social media site, many teens were uncomfortable with this practice [77]. Child and Westermann conducted a 235-participant survey related to parental Facebook friend requests, finding that teenagers generally accepted these requests out of obligation without making substantial changes to privacy settings [28]. In contrast, Cheng found that teens use a number of creative strategies to protect their online privacy, such as temporarily deactivating their Facebook account except when they decide to log in [27]. Forte et al. found that many high school students self-censor and maintain different social networks on different sites [39].

Teens are often more tech-savvy than their parents, leading parents to feel outmatched when attempting to monitor their children [120]. Wisniewski et al. conducted semi-structured interviews with ten pairs of parents and teens. Among their findings was that parental ignorance of technology could impede the parent's ability to engage meaningfully in the teen's online activity [135].

In contrast to much of this past work investigating teen privacy, we adopt a structured methodology that equally investigates the perspectives of teenagers and parents of teenagers. We rely on both perspectives to understand how parents make decisions about their children's privacy in a world that is far different from the one in which they came of age. We also document the extent to which our participants believe that teens have a de facto right to privacy from their parents in the absence of legal rights to privacy.

2.2 Methodology

We conducted semi-structured interviews with 20 participants: 10 teenagers and 10 parents of teenagers. Our study was approved by the Carnegie Mellon University Institutional Review Board.

2.2.1 Recruitment and Confidentiality

We recruited participants in and around Pittsburgh, PA by advertising a study on "privacy attitudes" at high school extracurricular activities, through word of mouth, by posting flyers, and on Craigslist. We recruited only teenagers currently attending high school (9th through 12th grade) and parents or guardians of teenagers within that range. To avoid potential biases of interviewing teens and parents drawn from different populations, we required that a teenager and a parent from each household both volunteer to participate in the study. In round-robin fashion, we then selected either the parent or the teen from each household to participate. Although interviewing a teen and parent from the same household would have been interesting, we felt that allowing other family members to know the precise topics discussed could lead to embarrassment or harm after the interview for participants, particularly teens.

Beyond interviewing only one member of a household, we took additional precautions to protect teen participants' privacy. Our recruitment documents and consent form were intentionally vague, noting only that the interview would cover "whether or not teenagers have a right to privacy" and what such a right would entail. We avoided choosing quotes for this chapter that we felt would identify particular participants. Furthermore, parents accompanying teens to the study were required to leave the interview room after completing the consent form. The audio recordings and transcriptions were password-protected and not accessible to anyone other than the researchers and transcribers.

8

We conducted interviews from November 2013 to March 2014. For their participation in our one-hour interview, we compensated participants $30 in Amazon.com credit.

2.2.2 Interview Procedure and Structure

Interviews were led by one researcher while at least one other researcher took notes and asked follow-up questions. The structure and topics of our interview scripts for parents mirrored those for teens. We began each interview by obtaining consent and explaining the study's purpose.

The topics of the interview included household demographics, technology practices in the household, and the decision-making process regarding the use of new technologies. We also asked teens about their digital personal space. To contextualize a participant's discussion about technology privacy, we also asked about each household's practices regarding physical privacy (e.g., the privacy of a teen's bedroom) and social privacy (e.g., parental notification when a teen goes out with friends). We concluded the interview by asking about teens' general privacy rights. Throughout the interview, we asked follow-up "why" questions for all responses that noted a privacy attitude or privacy decision.

We iteratively adapted our interview script based on previous interviews. The appendix contains our final interview script, which we used for the final eight participants (parents P7–P10 and teens T7–T10). In our initial script, we investigated digital privacy after physical privacy and did not explicitly ask about new technologies. We restructured the interview to emphasize our interest in digital privacy practices. We also originally asked questions about privacy laws, but participants' answers provided minimal insight into the research questions enumerated in Section 2.

2.2.3 Analysis

The researchers met multiple times during and after the interview process to review their notes and recollections of the interviews and to identify potential themes that warranted investigation in a more structured way during the coding process. These meetings also led to iterative updates to the questions asked in the interview in order to more fully investigate topics discussed by our earlier participants. After the final interview, the researchers met and collaboratively developed a draft codebook containing 88 codes within 15 categories based on their notes from the interviews and previous review meetings. For example, the categories of codes included reasons why teens have a right to privacy, areas of a teen's possessions that are considered off limits, techniques parents use to monitor their teens, and analogies used to compare the physical and digital worlds.

We transcribed each interview to facilitate coding and analysis. A research assistant used the draft codebook to code all of the interviews. We instructed the coder to modify or add codes as necessary to capture anything participants mentioned that was potentially relevant to understanding privacy attitudes or decision making. Following this first round of coding, the researchers and coder met to discuss the coded interviews. The coder had added one code, while eight codes and one category were never used. Realizing that some of the codes were ambiguous in practice, we added 27 additional codes in 6 additional categories. We deleted one category and ten codes, eight of which were never used.

Using this revised codebook of 106 codes in 20 categories, the coder went back through each interview and revised the codes. A second research assistant independently coded the interviews using the same codebook. The coders had 54% agreement (Cohen's $\kappa = 0.53$). The relatively low agreement appears to result from the large number of codes, some of which the coders felt overlapped conceptually. The two coders met to discuss discrepancies and reached consensus on all codes. We use these consensus codes in all analyses.

2.2.4 Limitations

Our participants are not a representative sample of the residents of Pittsburgh or any other population. However, our participants did come from a variety of cultural and socioeconomic backgrounds. Participants' families included teens in public, private, online, and homeschool situations.

Since we required parental consent for all teenage participants, we may have excluded teenagers whose parents were unwilling or unable to accompany their child to the interview. This restriction may have disproportionately impacted children of single parents or with troubled familial relationships. As our study was intended to obtain qualitative and anecdotal data from participants and not generalize to a larger population, we accepted this bias.

2.3 Results

After presenting an overview of participant demographics, we contextualize participants' privacy decisions by discussing their ideas about teens' privacy rights. Most parent participants felt that teens deserved privacy, albeit in a limited fashion. Surprisingly, many teens agreed that teens have only a limited right to privacy from their parents.

We then summarize participants' attitudes toward privacy in the physical world. While both parents and teens discussed providing notice before entering a teen's bedroom, most members of both groups felt that a teen's bedroom was not necessarily a private sanctuary. In fact, the benefits of parental laundry delivery appeared to outweigh privacy costs. However, as we detail in the subsequent section, teens considered text messages on their phones to be private, yet many parents felt it ethical for them to look through their children's text messages. In the final section, we unpack parents' decision-making processes, finding that in the understandable absence of technical expertise, parents made privacy decisions for their teens by drawing false analogies to the physical world or outdated concepts.

2.3.1 Participant demographics

We interviewed ten parents of teenagers (4 male, 6 female) and ten teenagers (4 male, 6 female). Table 3.1 summarizes participants' demographics. Our teen participants included 3 freshmen, 4 sophomores, 2 juniors, and 1 senior. All children in P8's household are homeschooled, while T3 attends high school online. The teenage residents of all other households attend traditional schools, including a mix of public, magnet, and parochial schools. We instructed parents to base their responses on their high-school-age children.

Two parent participants (P2, P3) and two teen participants (T2, T4) live in single-parent households due to divorces, while P4 is a widow. Both P5 and P6 live in two-adult households with partners who are not biological parents of the teenage children. All other participants live in two-parent households where both parents are the teenagers' biological parents. Two households (P8 and T3) had other children who attended college and spent most of their time on campus; Table 3.1 does not include these non-residents.

2.3.2 Teens' right to privacy from their parents

Most participants said that teens have some right to privacy from their parents. However, eight teens and eight parents expressly stated that this right is limited. Furthermore, nine teens and all ten parents indicated that parents would be justified in overriding a teenager's right to privacy

	Gender	Age	Grade	Children in household
P1	F	—	—	17/M
P2	M	—	—	14/M, 17/F
P3	F	—	—	4/M, 5/M, 6/M, 14/F
P4	F	—	—	14/F, 16/M
P5	F	—	—	12/M, 15/M
P6	M	—	—	15/M
P7	F	—	—	13/F, 15/M, 16/F
P8	M	—	—	14/M, 16/F, 17/M
P9	F	—	—	13/F, 15/M, 17/M
P10	M	—	—	12/M, 16/M, 18/F
T1	M	14	9	14/M, 16/M
T2	M	14	9	14/M
T3	F	15	10	15/F
T4	F	16	10	4/M, 13/M, 16/F
T5	F	18	12	18/F
T6	F	15	9	15/F, 17/F
T7	M	17	11	17/M
T8	F	16	10	16/F, 18/M
T9	M	16	10	16/M, 17/M
T10	F	16	11	16/F

Table 2.1: Study participants' demographics. Teens are identified by T and parents by P.

in an emergency. For example, P6 stated, "I don't know if that is a right or not...they are not necessarily required to share everything with parents... It's not like in the Constitution."

A few participants expressed more rigid views of teen privacy on both ends of the spectrum. Only one teen said that teens should have complete privacy from parents. P5 was the lone parent who agreed, saying, "Anything that they're doing in private is not really my business if they'd not want it to be, and I'm okay with that." Conversely, P2 acknowledged that his children would be surprised "that I feel I should have complete access" to their lives.

Why teens have a right to privacy

Participants, even those who did not think that teens had an overall right to privacy, volunteered many reasons why teens would have a right to privacy. As shown in Figure 2.1, common themes were trust and teens' inherent need for privacy. Participants also mentioned the importance of giving teens personal space, giving the teen respect, supporting the teen's comfort, fostering a sense of responsibility and independence, and acknowledging privacy as a human right. While seven parents mentioned reflections on the parent's own teenage years, only one teen mentioned this factor.

Ten parents and nine teens said that teens' right to privacy derives from parent-teen trust. In a representative response, T3 said his parents respect his privacy because "they trust me a lot." P4 discussed the importance of earning trust as a prerequisite to earning privacy, explaining, "It's a matter of making me believe in you, making me trust you."

Five parents and three teens said privacy was a human right deriving from dignity. Parent
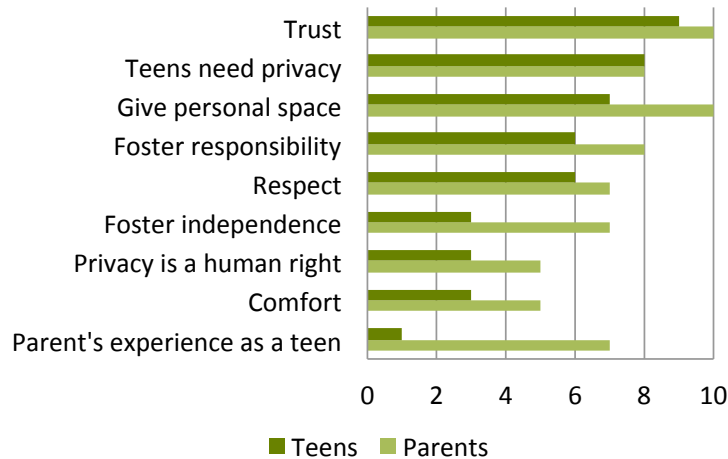
Figure 2.1: The number of parents and teens interviewed who mentioned each reason why teens should have privacy from their parents.

P5 ardently expressed this belief, saying of her sons, "Teenagers are people and everybody has the right to privacy. And just because I gave birth to them and parent them and am responsible for them, doesn't mean that I get to control everything about their lives. Part of teenager-hood is going apart and finding your boundaries, and if I don't let him have any boundaries separate from me, then it's going to make it a lot harder to find his own person...It will affect his life in detrimental ways."

Six teens and seven parents suggested granting privacy was a sign of respect. P3 tied respect to her own experience when she said, "I believe that we should give our kids certain signs of basic respect as is age-appropriate. So if I see [my daughter] is healthy and well-functioning I don't see a need to just go into her room arbitrarily. Just like when I was a teenager I didn't particularly like that."

Why teens do not have a right to privacy

Participants also noted reasons why teens should not have privacy, as shown in Figure 2.2. Common reasons were a parent's "right to know" and parents' concerns, particularly safety concerns. Participants also said that teens have nothing to hide, teens who depend financially on a parent are obligated to share information, and that teens of a particular gender are more vulnerable and thus do not have a right to privacy. Six parents mentioned that teens in "my house" do not have a right to privacy, four parents mentioned that a parent's own transgressions as a teenager compelled them to look into what their teens were doing, and seven parents mentioned that taking away privacy rights was important when they needed to teach their teen a lesson. Notably, no more than two teens mentioned any of those three reasons.

All but one parent and one teen concurred that parents had a right to know things about their teens because of parental responsibility. P2 felt it ethical to view his children's devices and accounts based on his responsibility for their welfare. He explained, "You're responsible as a parent for them... You need to be aware until they turn 18." P8 stated more generally, "Teens do not have a right to privacy [because] parents are still responsible for their children."

Seven teens, along with eight parents, expressed the need for parents to limit teens' privacy when safety was at stake. P6 displayed reluctance to look through his son's messages unless he
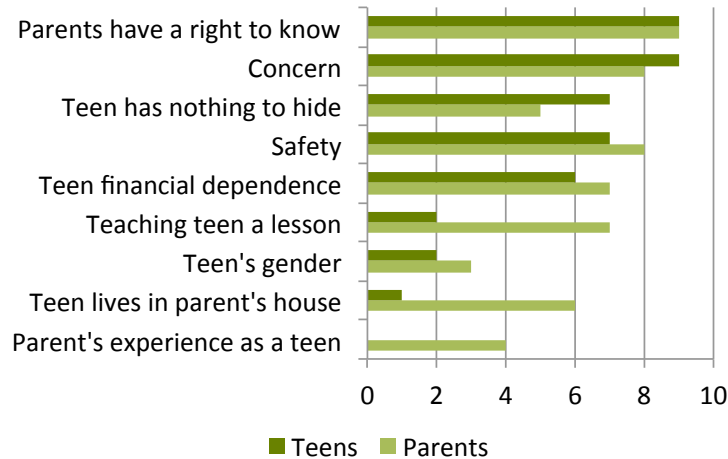
Figure 2.2: The number of parents and teens interviewed who mentioned each reason why teens should have limits to their privacy from their parents.

was concerned about his son's safety, saying, "I would need to really feel like that violation of his privacy was outweighed, you know, that his safety was more important."

The question of who was paying the bills was also important in determining privacy rights. Six teens and seven parents indicated that teens' financial dependence on their parents minimizes their right to privacy. T7, T9, and T10 all echoed that when parents pay for a teen's education, they have a right to know how the teen is performing academically. P1 expressed dismay that FERPA would bar access to her son's grades once he turns 18 even if she pays for his education. She said, "I think that's wrong... If the parent's paying for it, I want to know what's going on."

Financial dependence also drove the sentiment expressed by six parents that, because teens live in houses owned by their parents, they have fewer privacy rights. T8 said, "It's their house, so they can do what they want." Similarly, P2 expressed his right to enter any room in his own home: "It's my house...If I need to go in there, I'm gonna go in."

The boundaries of privacy rights

Nearly all parents noted boundaries to teenagers' privacy rights, often explaining that these boundaries are fluid. P6 wrestled with these limitations: "I will do my very best to honor [my son's] privacy, but if at the end of the day I need to do something that violates [his] privacy because I feel like it's the right thing to do... then I will violate the shit out of his privacy... That's my responsibility as a parent."

P4 explained the difficult balance between privacy and control: "At one point [my son] called me controlling. I don't think I'm controlling. I think I'm protective." She expressed her struggle by saying, "I wanted to...not be controlling, but I still wanted to have some control."

Some parents noted areas as expressly permissible for parents to access. Both parents and teens commonly noted grades in school as non-private. P7 was dismissive of teens keeping grades private: "Grades? No, that's not privacy to me." Many teens noted that their schools automatically shared grades with parents and that they had neither the ability nor the right to keep grades private from parents.

Parents also noted situations they would consider violations of their children's privacy. P2 said, "If my daughter likes some boy at school and she doesn't want to share that with me, that's fine."

Similarly, P5 described why looking through her sons' digital files was inappropriate: "I don't think there's any reason to. I mean, if the teenager agrees to it, but only then. And that's often questionable because I think it can be very easy to coerce them into agreeing."

While many parents reserved the right to override teens' privacy rights, our interviews suggest they do so infrequently in practice. Asked whether she has the right to read her daughter's correspondence with friends, P3 said, "I do, but just because you have the right to do something doesn't mean that it's morally the right thing to do."

Age, maturity, finances, and college

Participants noted that privacy rights are not static. They commonly felt older teens should have different boundaries and privacy expectations. Privacy rights evolved based on age, maturity, financial independence, and starting college.

Privacy rights increased with age according to seven teens and all ten parents. P2 described how his practices changed as his children grew older: "I, as time went on... allowed them to make their own choices." Six parents and six teens also mentioned maturity. P7 explicitly distinguished maturity from age, saying, "It really depends on the maturity of the kids. And not necessarily the age."

Participants had nuanced views around privacy changes when teens turned 18, the legal start of adulthood in the United States. T5 acknowledged the legal boundary at age 18, saying, "I think when you turn 18, your parents even owe it to you in a way to give you more responsibility." P4 also acknowledged this boundary, saying, "He's going to be eighteen, so I don't really have any say at that point." However, she also lamented, "I think eighteen is young." Surprisingly, few parents or teens expected that teens should obtain full privacy rights on their eighteenth birthday.

Six teens and eight parents cited increasing financial independence as a factor impacting privacy rights. P4 indicated that she would give her son more privacy when he started financing his own phone: "At some point he's going to pay for his own phone and stuff, and... there should be trust there so I shouldn't have to look at it."

2.3.3 Privacy in the Physical World

Parents were generally willing to carve out private space in the physical world for their children. Privacy in the physical world did have its limits, though. P1 directly addressed the superficial tension between teens and parents regarding rules: "There's some resistance, but I know in the end [my son] appreciates me and loves me for it."

We found that parents generally let teenagers keep the door to their bedroom closed, except when significant others were visiting. All parents felt entitled to enter their children's rooms when their children were not there. As long as parents were not snooping, most teens agreed. Teens appeared to consider few physical areas private. Most parents had rules and restrictions about their children's social lives. All teens were required to notify their parents of their physical location at all times. While these requirements did cause some parent-teen tension, both parents and teens generally agreed that such practices were reasonable.

Bedrooms

We found that parents generally treated teens' bedrooms as somewhat private, giving the teens personal space, yet did not feel like they should be restricted from entering. While teens did not approve of the relatively rare practice of parents snooping around their room, they felt that the
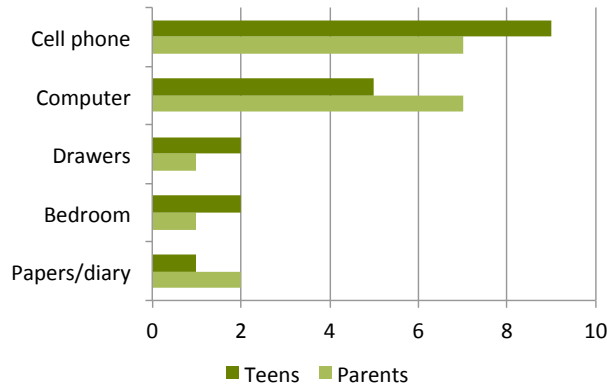
Figure 2.3: The number of parents and teens who said different areas were inappropriate for a parent to go.

benefits of having their laundry or other tasks done for them were valid reasons for their parents to enter their room.

We found wide acceptance of the practice of teens keeping their bedroom doors closed for privacy. P2 said he permitted his children to keep their bedroom doors closed because "that's their space." A few parents gave their children privacy in their bedrooms, yet explicitly noted that they would still go in if they wanted to. As P3 explained, "Mom reserves the right to check on any of her children at any time."

All parents and all but two teens indicated that parents knocked or otherwise notified their children before entering their room. Respect often drove this decision; P1 explained, "It's his private [space], it's his domain. Well, not domain, but just out of respect. I'd expect the same." Generally, parents and teens used knocking or other advanced warning to avoid awkward situations. For instance, P5 explained, "Since the door is closed, there are potential things I could be walking in on that neither of us want to know about."

All parents felt comfortable entering their children's bedrooms when their children were not there, and all teens except T4 said their parents enter their room when they are not there. None seemed particularly troubled by this practice as long as their parents had a reason. For instance, T7 felt it was acceptable for his parents to come in "to get my laundry. That's pretty much it. Or make my bed."

A handful of parents interviewed did think it appropriate to snoop through children's rooms. P1 noted that she enters her son's bedroom multiple times a week "to snoop. It's my house and I'm gonna go in that room whenever I want to." Despite this snooping, she did not feel like she was violating her son's privacy. She explained, "Hell, there could be a mad man living in the room, how would I know? I could see Dr. Phil, 'Well, you never went in your son's room, huh, would you now?' Ya, I respect his privacy, yes I do."

Although most parents and teens generally considered unprovoked snooping a privacy violation, only a few participants felt particular areas of the physical bedroom should be off limits to parents. Some parents who mentioned specific locations noted that these policies were hypothetical. For instance, P1 said "if [her son] had a diary, I wouldn't look through that." No participant other than P3's daughter actually kept a diary.

Instead, both parents and teens most commonly mentioned cell phones and computers as off limits to parents. Seven parents each mentioned cell phones and computers. While nine teens mentioned cell phones, only five mentioned computers. Figure 2.3 enumerates the locations and

devices participants suggested were off limits for a parent.

Privacy in teens' social lives

All participants except two parents and three teens noted that the teenagers in their household had restrictions on their social lives, most commonly curfews or restrictions on overnight visits. Whereas T10 was representative in saying "[My mom would] never let me sleep over at a guy's house, or let a guy sleep over at my house," T4 was similarly representative of the flexibility most teens created for themselves, saying, "Oh yeah, [I violate my parents' restrictions] a lot. I'm always late on curfew."

All participants, even those without restrictions, noted that the teens in their household needed to notify their parents in advance about where they were going. There were some complaints about required notification, but they were limited. P1 discussed her son's objections, saying, "He says I'm always calling him... And he wants his own personal space." Surprisingly, all of the teens we interviewed felt the notification process was reasonable, though annoying.

We also investigated attitudes about teen dating and romance, particularly concerning privacy. While participants had a range of views on the appropriateness of teen dating, these discussions provided little insight into privacy decision making. Most commonly, parents wished to be oblivious to their children's sex lives. As P4 said, "It makes me a little bit 'ew'...I'm not sure that I want to know." P1 explained, "I don't even want to think about it...That's disgusting."

2.3.4   Teen Privacy in the Digital World

We investigated teens' attitudes towards digital devices, including laptops and phones. Teens largely expressed that their digital spaces were personal and private. We also note the prevalence of teens using laptops solely for schoolwork, rather than recreational browsing, as well as the prevalence of teens using texting as a primary communication channel.

Devices

Teens felt strongly that phones were private devices that parents should not access. In contrast, laptops were less private and primarily for schoolwork. T9 said, "People don't have the right to go through [my phone]." Similarly, T2 expressed annoyance at his parents "constantly searching my phone," which he thought demonstrated a lack of trust. P9 was aware of the value her children placed in phones, stating, "no one should be in each other's phone...invading other people's rights." Few teens used computers for socializing. T8 spoke for many of our participants when she said that phones were "more private" than computers.

Many participants relegated laptops and personal computers to schoolwork only. As T5 explained, "A lot of schools will provide you with a Chromebook or something of that sort." This led some teens to distrust the school-provided laptops because, as T4 put it, "I think that they can go in and check [my activities]." As a result, many teens chose not to use their computers for anything other than schoolwork. T7 said, "I don't really use my laptop that much, just for like schoolwork and stuff like that." T8 concurred that her computer was used for "mostly school," while T10 stated that "the computer just has school documents on it."

Most parents also observed that computers were primarily for schoolwork. Of her son's laptop, P2 explained, "He hardly ever uses it, except for schoolwork." Monitoring and content-control software on school laptops seemed to be a significant reason for teens' minimal use of laptops. As P5 describes: "my older one has a school provided laptop that is very locked down, and he really only uses it for school."
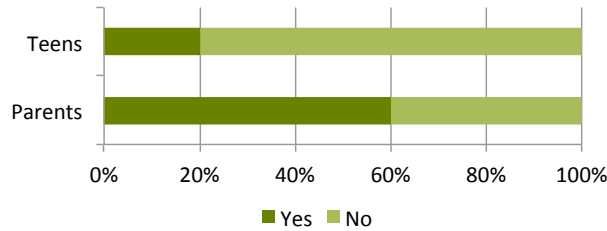
Figure 2.4: The percentage of parents and teens who felt it ethical for parents to look through teens' text messages. Teens strongly opposed this practice.

Texting

Many teens used text messaging for private communication. Our teen participants repeatedly echoed this thought, with T2 saying, "[Parents] looking at my texts...feels like an invasion of privacy," and T10 explaining, "Texts are more private because that's where I talk to my friends."

Some parents had also observed that teens relied on texting for private conversation. P9 observed that her children "use their phones for socializing and I don't feel the need to get involved in that. And they don't want me to." However, many participants said that parents in their household had no qualms looking through text messages, such as when T2's mother punished her son by looking through his texts. He explained, "I lost her trust and she decided to look through all my text messages on my phone." In some households, parents monitored teens' texts even more regularly. P10 and his wife routinely checked their children's phones for "texting, anything they can access with that," and he expressed that he would prefer to be "checking [texts] more consistently." While many parents felt it acceptable to monitor texts, very few teens agreed, as illustrated in Figure 2.4.

Social Media

In general, teens' reported interest in traditional social media seemed to be waning compared to past studies. We asked specifically about teens' use of Facebook. Signing up for an account often came "with the provision that if you have a Facebook account, you friend your parents," as explained by P8. Perhaps in reaction to this, teens had moved away from Facebook for personal activity and correspondence. Besides running a few group pages and talking to family, T3 admits, "I don't really do anything on Facebook besides just like, checking every once in awhile." P6 observed, "I think that Facebook is kind of trending away with the younger generation, especially when his parents and all his parents' friends are on there."

While few teen participants said they regularly used Facebook, many of them did report using Instagram, Snapchat, Vine, and Twitter. However, teens' shift from Facebook to these new services was not yet on most parents' radars. None of our parent participants were familiar with Instagram or Vine, while only one (P6) had ever heard of Snapchat. P6 was not sure, however, whether his son used Snapchat.

2.3.5   Decision making

In this section, we first examine parents' decisions about monitoring and restricting their teens' use of technology as examples of privacy decision making. We then unpack parents' decision making about their teens' privacy. We discuss how parents rely on their own experiences as a teenager to
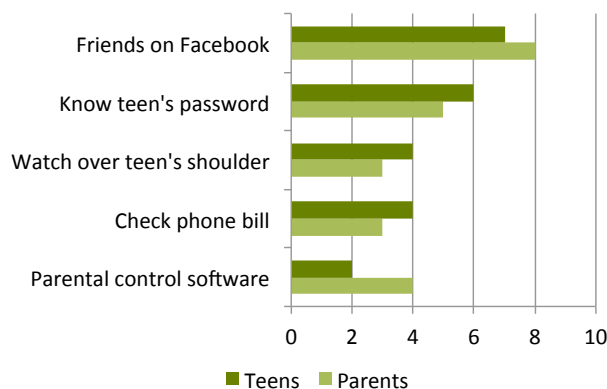
Figure 2.5: The number of parents and teens we interviewed who reported the adults in their household employing different types of technological monitoring.

make parenting decisions about technology, even though participants thought today's world differs substantially from the world of 25 years ago. We also evaluate the extent to which participants conceived of privacy similarly online and in the physical world, which was a source of parents' misunderstandings of how private teens consider their devices.

Decisions about monitoring

Parents utilized a variety of methods to monitor their teens' online activities. As shown in Figure 2.5, parents commonly relied on being Facebook friends with their teens, knowing some of their passwords, or looking at their teens' phone bills. Some parents placed computers in public areas of the house to watch over their shoulders, while others surreptitiously monitored teens' activities. Four parents and two teens reported that parental controls had ever been used in their family, while four parents (P1, P6, P9, P10) simply required their children to show them their devices.

In a few households, computers were kept in a public area so that parents would know what their teens were doing. When describing her 14-year-old daughter's computer use, P3 stated, "Her computer's kind of in a public room where mom can see." T1 described how his parents would observe by listening, saying, "Sometimes they come and just stand there and they don't say anything. Normally, they're just listening to my Skype conversation." A few parents also monitored surreptitiously. For instance, P7 said, "Sometimes it happens that I check [my kids' browsing] history."

Four parents and two teens mentioned parental control software. P8 used parental controls primarily to restrict certain content, but had dabbled in blocking social media: "Basically it was a filter for, just, stuff we thought might be offensive sites...earlier on we kinda limited some social networking, because we wanted to get a sense of who they were communicating with." Notably, however, most of the families that had used parental controls had since abandoned them due to the frequent false positives. In other cases, the families had no idea whether the parental controls were still active. A few participants reported using parental controls on mobile or portable devices. T9 had struggled against restrictions on his iPod, recalling, "[My Mom] put a password on it to sort of change the restrictions [to prevent downloading explicit songs], so I tried to guess it; successfully, eventually, but by then it didn't really matter."

Parents often paid for teens' cell phone plans, so some had access to records of whom the teen had called and texted through the monthly phone bill. Many parents took advantage of this and

reviewed the logs (P5, P6, P7). As T3 reported, "They check which numbers I text." For the most part, teens assumed that parents were primarily monitoring not who the teen contacted, but that teens were not staying up too late (T3 and T9). In T2's case, his mother, who lived separately, looked at his phone bill to ensure that he was not ignoring her. He said, "[If] I haven't talked to her in a couple of days...she checks the phone bill to see if I've been texting people and calling, to see if I'm ignoring her."

Some parents looked through teens' text messages. P5 did not do so, which she felt made her an outlier. She explained, "I have many many friends who have, say, teenagers or pre-teen kids who do think it's absolutely acceptable to take their phone and look through their kids' messages, or limit things, or just read over emails." T4's father would frequently look through her text messages. She developed a strategy to avoid her father's prying, saying, "I leave [my phone] in my room and I'll just tell my dad I forgot it."

A common practice was for teens to be friends with their parents on social media, often as a condition of using the site. As T6 put it, "I'm friends with my parents on Facebook. That's, like, a big thing." P10 dryly remarked of his children, "Yes, [my wife's] on Facebook, much to their chagrin." However, not all teens friended their parents under duress. P6 described his son's Tumblr use, saying, "My girlfriend is a follower of his on Tumblr. And he follows her. It's very out in the open. We're not sneaking up on him."

Five parents and six teens reported parents having access to teens' passwords. Motivations for this practice differed. Sometimes, passwords were necessary to maintain the computers. As P8 explained, "When I need to go in and manage their side specifically, I log on with their password." Monitoring content was a prominent goal for other parents. P10 and his wife regularly checked his teens' computers, using their passwords for "checking for online searches, checking email, Facebook, social networking, that sort of thing."

Many parents reported having access to passwords, yet not using them. T10's family keeps a written list of passwords that all members of the household can access. Some parents helped teens set up computers or accounts and had their teens' passwords as a byproduct of that process. For instance, P5 said, "I did help them set up their Gmail accounts years and years ago. They probably haven't changed their passwords, so I probably still have them. But I haven't logged in in five years or whatever." P3 explained having her daughter's password was a safety measure, saying, "I just have the password. To me it's kind of a safety thing. I have jumper cables in my car...I hope not to have to use them tonight, but they're in there just in case."

Deleting information, such as browser history or text messages, was a common tactic among teens to avoid exposing private content to parents. Surprisingly, a number of parents expressed that they wanted their teens to delete things. For example, P4 lamented, "I'd think to myself, why didn't you delete it?" Teens expressed that they tried to be clever about covering their tracks. T4 explained, "I try to delete some of [my text messages] so it's not really obvious." Managing and routinely clearing questionable data took a toll on some participants. As T9 admitted, "I've watched pornography...At the time that I did, I was really a lot more paranoid about search history and stuff."

Decisions about restrictions

When parents attempted to regulate teens' technology use, they turned to non-technical methods. Parents sometimes took devices away, imposed time limits, or specified where devices could be used. As punishment, parents took away devices and shut off Internet access. When P9 wants to discipline her children, she "will take the phones away when I feel they're acting disrespectful." As T6 admits, "My dad turned the Wi-Fi off my house at one point." Parents usually imposed time

limits verbally. T10 explained, "We'd play games and they'd say, 'Okay, only 15 minutes."' Other families required devices to be used or not used in certain areas of the house. T6 explained, "They don't usually let us have laptops in our rooms."

Parents' own teenage years

In determining what policies to set for their teens' privacy, parents commonly used their own experiences as teenagers. For instance, P1 explained, "I try to think back when I was his age." She actively gave her son some private space, even though she decided that snooping in his room was not a violation of his privacy. On the other hand, P5 explained that she emphasized being open with her children, lamenting that her mother "never started the conversations."

Other parents mentioned their own transgressions as informing their parenting decisions. For instance, P6 said, "When I was fifteen, I totally would have broken all those restrictions." Similarly, two other parents mentioned their experiences as teenagers hiding marijuana from their own parents. Amusingly, P4 lamented her own children's inability to hide their tracks, saying, "These kids today. When I snuck out of the house at his age, I made sure that I came in and left and didn't get caught!"

Differences today

While parents' own experiences are crucial to their decision making, all participants noted many ways in which being a teenager today is different than it was 25 years ago. In addition, except for P8, all parents said their view of teen privacy is different from how their parents viewed it when they were teenagers themselves. Technology played a major role in these changes, and the use of technology was starkly different. For instance, P6 mentioned that his son started using a computer at age 2. In contrast, he said, "When I was fifteen, we had an Apple IIe computer at home...I honestly couldn't do anything with it."

The most salient difference was a tension relating to teens' freedom. While modern teens have the freedom to access huge amounts of information, they lack the freedom to disappear from their parents (P1, P5, P7, P9). The expectation is that they are always connected. As P4 explained, "I have to know where he's at. If I call him he has to answer." Similarly, P5's kids had "just gotten smart phones and one of the agreements for that was that I need to be able to get in touch with them whenever I need to." Some teens were cognizant of the implications of cell phones. As T5 said, "There comes a lot with a cellphone, in the sense that you can be reached at any time. Or be bothered."

Parents contrasted modern expectations of constant availability with their own childhoods. P7 reminisced, saying, "My parents didn't know where I was for hours...I couldn't call." Similarly, P9 recalled, "I'd say I'm going to New York...[and] come back like eight hours later. Did they ask where I was, what I did? No! I was back."

For many parents, technology thus became a means of control (P4, P5, P6, P7, P9). P7 explained, "The reason why we both have the phones is because we parents want to actually control them. So, at least 50% of the reason was for us, not for them." P6 focused on the use of technology in schools to keep tabs on his son. He said, "Thank God for technology...I do look at his grades and his missing assignments...It's kind of like that whole panopticon thing."

Some parents felt technology has made teens' lives much more complex (P4, P9) and dangerous (P2, P7, P10). P10 said, "There weren't as many issues as there are today for teens for a privacy issue to arise...The biggest problems in schools were chewing gum, and these days it's weapons and drugs and rock & roll, alcohol." Teens tended to be somewhat dismissive of this viewpoint. T8 explained, "When my parents were my age, they tell me about how they walked everywhere and
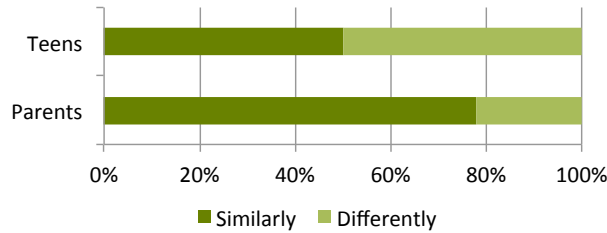
Figure 2.6: The percentage of parents and teens who said they think similarly or differently about privacy in the physical world and privacy online. We exclude one parent and two teens with whom we did not discuss this topic.

how they could keep their doors unlocked and we can't do that today." When asked why this was no longer the case, she snarkily replied, "Because I could get abducted or something, I don't know." T9 instead characterized the generation gap as one of access. He said teens now "do things much more efficiently, like setting up a party...It's kind of like what they had, but for us it's on steroids."

Some parents (P2, P5, P6, P7, P9) expressed shock at the extent of teens' lives that occurs online. As P6 explained, "[My son] spends a significant portion of his life online. He really does. And I think most kids do." He contrasted this state of affairs with his own childhood: "The things that were private when I was fifteen were my bedroom and what was going on in my life." Teens also recognized parents' confusion at the way teens communicate. For example, T8 said, "They think it's weird that I'm on the computer a lot, but it's just something that this generation does."

One parent noted that people her age are the first to have experienced stark generation gaps between parents and teens. P9 explained that, for her own parents, "the big thing [for my parents]...was like smoking and drinking and playing cards...I think that their lives were so similar to their parents' lives, like there wasn't a big culture break...I was educated in a lot of the liberal views and sexual freedom...Honestly, I was a lot wilder than my kids ever will be." She drew another distinction with her children's generation. She said, "I worked from age 12 because life was boring...[Now] I feel like we can do so much with a phone: we can look up, we can research, we can read books, we can talk to people." As a result, she had to kick her "oldest son's butt to work and he's like 'Why? I have a phone. I have access to a car. I have friends. I get good grades. Why would I need to work?"'

Online vs. physical

A large part of the gap between parents' and teens' privacy decision making process appeared to be predicated on whether they thought similarly about privacy online and in the physical world. Excluding three participants who did not discuss this topic, 7 of 9 parents said they thought similarly about privacy online and in the physical world, whereas only 4 of 8 teens said the same (Figure 2.6). It is less surprising, then, that teens and parents differ in opinion about privacy for digital devices.

Many parents felt that the human characteristics underlying the physical world applied equally to the digital world. P3 explained, "I didn't have a cell phone. I didn't have Internet back then. It was kind of like a different world. But as far as respect goes, basic respect is always gonna be basic respect." Similarly, P6 offered, "Just because they're not sitting in front of you doesn't give you the right to talk in a way that you wouldn't talk to someone who was right there in front of you." Other parents had not given potential contrasts between the digital and physical worlds much thought. When asked detailed questions about parenting practices, P2 was surprised to conclude, "It seems

that I do give them more space online than I do physical."

P6 drew a direct parallel between his son's privacy in the real world and online. Early in the interview, he mentioned his son had a small chest in his room. P6 said his son "had a lock on it for a little while, not actually locked, just kind of hanging on the thing. It was an interesting symbolic demonstration of 'this is off limits,' even though it clearly wasn't, because anybody could just take the lock off." P6 chose to treat the chest as his son's private space and not snoop. When later discussing how he knew his son's computer passwords, P6 explained, "I want the password in the same way that I [would] want a key to the lock on his footlocker...I'm not going to snoop around in his stuff...[But] if I had cause to think I needed to look at that stuff, I want to be able to do so at my convenience."

P7 also drew parallels between her son's behavior on the computer and her experiences as a teenager in the physical world. When her son deleted his computer's browsing history, P7 found it "really smart but also suspicious. I mean, you clean the history because you want to hide something. But then I had a second thought and I said, well, I tried to actually create a similar situation when I was a teenager. I remember that I wrote down notes, not really a diary, but some kind of personal notes. And I could have hated my parents after reading that stuff. So I try to respect this kind of private life for whatever it is."

Interestingly, the parents and teens who distinguished between privacy online and privacy in the physical world had diametrically opposed views about the relative danger of these contexts. Parents felt that the physical world was filled with friendly faces, yet online was filled with strangers. P5 explained, "My concern for privacy online is much more of protection from other people...Like if they close their bedroom door, the only risk to me looking inside is that I'm looking inside. Whereas if they have a Facebook account or whatever, and they don't close the door properly, then a billion people can look inside." P7 similarly asserted that online, "your stuff is available or reachable by a much bigger context. So if you publish something, it's not just your circle of friends or family, it can really go to the world. So the impact is ten times, one hundred times bigger."

In contrast to the parents, the teens we interviewed felt their online world comprised their friends, whereas the physical world was inhabited by strangers. As T8 explained, in the "physical world, the majority of the people I see are strangers, so I don't really worry about them thinking about what I'm doing. But online, like the people that follow me, I know them personally. So I think what I do will kind of affect them more in how they see me."

The teens we interviewed also had trouble understanding the online dangers their parents emphasized. In fact, the teens felt that there were fewer possible consequences online than in the physical world. T7 explained, "If someone finds out that you did something in life, you can get in trouble at school or get in trouble with your parents or something like that. But online, there's not that much stuff that you can get into trouble." With one exception—T5, who noted concerns about online hackers and cyberbullying—the teens felt that their school assemblies about online safety were excessively alarmist. T8 characterized the latest such assembly as "kind of boring, so I kinda like just zoned out." As a result, teens felt that parents misunderstood the decisions they were making about online safety.

The teens did note some exceptions to the general safety they perceived online. T6 noted that, in the absence of actively deleting information, "online stays there forever." Furthermore, teens made a specific exception for Facebook, which they felt was the one area where their online life intersected their life in the real world. T10 said, "It makes sense to me why [my mom would] want to monitor my Facebook because people talk about how when you're looking for a job they'll look on your Facebook."

Misunderstanding teens' private spaces

One major disadvantage parents had in their decision making process was an incomplete under-standing of the technologies their children were using daily. Half the parents we interviewed said they struggled with technology (P2, P4, P5, P7, P9). P4 told us she "just realized that you're able to go online" with gaming consoles. Describing Android unlock patterns P6 said, "I watch him do it sometimes and I still don't understand." P2, who works in the tech industry, explained that the mother of his children was reluctant to let the kids have email accounts because she is "more paranoid about things she doesn't understand." Yet he also struggled when trying to comprehend his son's "36 virtual friends."

Unsurprisingly, teens then felt their parents failed to understand modern communication. T6 lamented, "They think that you're behind a screen, so you're cutting yourself off from the world. But I don't think that. I think you're talking to people." This tension clearly manifested itself regarding text messages. Whereas T5 happily noted texts as the default communication channel, P1 complained that texting "makes me mad. I want to hear [my son's] voice."

Beyond teens' reliance on text messaging, the parents we interviewed struggled to understand the private nature of those conversations. For instance, even though T6 often deletes text messages, she said, "[My parents] want me to think before everything I write, even in a [text] message." The impermanence that teens attributed to phone conversations carried over to apps. Even though she was aware of the ability to take screenshots, T6 considered Snapchat to be her most private method of communication. Only one parent (P6) had heard of Snapchat; none had ever used it.

Whereas teens relied on the ability to delete messages on the phone, parents felt that digital communications were uncontrollable once sent. P10 said text messages "can be forwarded. They can be copied. Other people can find out about them." He felt that the only type of private communication between friends was "a written note [or] getting alone with them [in a] room... the old fashioned ways." Similarly, P3 believed teens communicate privately via notes, as was the case during her childhood. She said, "Teenage girls, I was one of 'em once, pass notes to her friends in her school." As a result, she did not consider her daughter's phone to be private and had configured her daughter's phone to communicate only with whitelisted numbers.

Some of parents' unfamiliarity benefited teens. T8 explained, "My dad, he's bad with technol-ogy. But my mom could adapt if she wanted to. I don't think she really cares to... She mostly just pays attention to Facebook," which was convenient for teens since none of our teen participants considered Facebook to be particularly private. In contrast, T8 thought it "would be weird" if her mom wanted to follow her on Twitter. Similarly, T10 happily mentioned, "I don't even know if my mom knows what Snapchat or Instagram is."

A major difference we observed between parent and teen participants was their understanding of what types of private spaces were most essential. Most parents thought allowing their teenagers to be alone in their bedrooms with the door closed was sufficient private space. Putting herself in her son's shoes, P1 said, "This [bed]room is my world. I can listen to my music, go on the computer, do what I want." P5 noted that "everybody needs a space that they can go to that they can just be private... Since the house is mine, the bedroom is really the only space [teenagers] have." By a similar thought process, P6 noted carefully avoiding looking "under the mattress" when he needed to search for bedbugs in his son's room because "when I was a child, that was a place where you hid things away from your parents."

However, teens generally did not hide things under their bed; they hid them in their phone. Many of the parents we interviewed did not grasp the importance of cell phone privacy for teens. Even P6, who generally felt "it's not ethical to go through anybody's text messages [because]... it's the equivalent of digging through somebody's drawers," struggled with teens' phone privacy. He

later noted, "if the day comes that I really want to look at his phone, I could."

Parents' struggles evaluating privacy

In the end, all but one parent said they struggled making privacy decisions for unfamiliar technologies. When asked how he decides what rules to adopt for new technologies his son is using, P6 said, "I kind of make it up as I go along." He further explained that his son "has access via the Internet to things, materials—explicit materials in particular—that when I was fifteen, you just didn't have access to... And that does pose a problem in terms of what does that really mean? But that's an answer that I don't have."

The lack of context caused particular difficulty. P8 simply noted that "the playing field is different." This different playing field left parents unable to evaluate risk; P7 complained, "How can you compare? Like my kids can actually be in the dining room and chatting with somebody in China... The reality is they could actually be in more danger."

The rapid pace of change was an additional confound. P10 explained, "You're comfortable with what you're familiar with. And today things are changing so much that it's hard to get familiar and comfortable with something because there's a new advancement something's new and improved, or there's a whole new way of communicating." Similarly, P4 lamented, "It's overwhelming for me... It's so different from when I grew up... I don't know if I'm too strict or too loose."

2.4 Discussion

Our interviews with ten teens and ten parents delved into how parents understood and navigated teens' privacy in an unfamiliar world, as well as how teens perceived their parents' decision making. Our findings unveiled a notable disparity between teens' and parents' views of technology, cutting across family dynamics and socioeconomic classes.

In some areas, we found accord between parents and teens. Both groups generally acknowledged that teens had some right to privacy from their parents and that this right was limited. However, as we look toward real-world examples of privacy rights, parents and teens begin to diverge. Many teens felt that their smartphones, containing text messages and apps, were their most personal form of communication. Even when the parents we interviewed expressed a desire to give their teens personal space to socialize with their friends, they anticipated the teens would have an in-person conversation, not use text messaging. As a result, these parents often adopted policies regarding use of technology that clashed with their abstract goals of giving teens private space.

Despite their conflicting perceptions of technology use, both parents and teens were operating in good faith. Communication problems were the heart of the issue. Parents struggled with how to make decisions about technology use—they weren't intimately familiar with many of the technologies and made incorrect assumptions. Meanwhile, teens were more familiar with the technologies, but were not always able to make responsible and mature choices. In one example, parents frequently required that their teens friend their parents on Facebook as a condition of signing up for the site. While parents felt this was a good way to keep tabs on their children's digital activities, it seems to have caused the teens we interviewed to stop using Facebook regularly. Instead, teens overwhelmingly preferred texting, Instagram, or newer apps for socializing with friends.

The communication gap arising from generational differences and differing perspectives on the role of digital devices and the Internet is a substantial obstacle to parents' decision making. We intend this chapter to inform the conversation about how to help parents make privacy decisions for their teens in this technology-filled world that differs starkly from their own childhood. While

we did not test specific approaches, our results provide insight into the needs of parents and teens that can help guide developers.

Even though many of the parents we interviewed described struggling with making decisions about privacy for their teens, few of them regularly used parental controls or other digital parenting software. Even the families that had used these tools in the past reported that the trouble of using them often outweighed the benefits. One reason for this non-adoption might be that the tools do not support parents' goals sufficiently. Existing digital parenting software most commonly blocks access to resources deemed inappropriate according to some heuristic. Frequent false positives in this blocking cause frustration and lead parents to disable these parental controls [121]. Other tools are designed to notify parents about their children's activities, such as their location. However, parents sometimes find this approach stifles their children's independence and maturation process, again leading to non-adoption [123].

Our results suggest that there is ample opportunity for tools that inhabit a middle ground between doing nothing and forcibly preventing or conspicuously reporting teens' actions to their parents. Parents who are concerned that they are not doing enough to teach their children to make responsible, privacy-protective decisions when using technology might find value in software tools that encourage, rather than force, certain types of behaviors. This approach of encouraging, or "nudging," users to give more careful consideration to a decision has been applied successfully to a number of domains [12, 125].

Among digital parenting software tools, this approach to software might use heuristics to detect actions that a parent might not approve of and take the opportunity to remind the teenager of the parent's expectations and the teen's responsibilities, yet not block the action. For example, in a field trial of privacy nudges for Facebook, Wang et al. found that visual reminders of a family member being able to view content was effective in encouraging privacy-protective behaviors [124]. The nudging approach to digital parenting software might alleviate parent-teen tensions because teens would still be free to make their own decisions, albeit with guidance and reminders.

Our results can also inform efforts to improve user education around these new technologies. In particular, we observed a major gap in parents' understanding of how their children use new types of devices, apps, and services to communicate with their friends. Unfortunately, much of the discourse in the popular media about these new technologies focuses on worst-case scenarios. Instead, parents might benefit from a better understanding of how the majority of teens actually use apps like Snapchat, beyond the fact that a fraction of teenagers use it to send explicit photos. Similarly, the increased understanding of parents' and teens' perspectives that we provide can be used to improve laws like the Children's Online Privacy Protection Act of 1998 (COPPA). While other scholars have noted flaws in the implementation of COPPA [82, 17], our additional perspective can help suggest potential next steps in improving privacy laws.

In our next chapter, we expand upon the privacy and safety tensions discussed above through interviews and surveys of online safety professionals, parents, and teens. We examine parenting strategies in order to understand how teens, parents, and professionals think about effective ways of keeping children safe online.

2.5   Acknowledgments

Chapter 3

Digital Parenting: A Comparative View of Strategies, from Expert, Parent, and Teen Perspectives

Teens are using the internet and digital devices for many hours every day [65] as their main outlet for socialization [16]. Because parents of teenagers did not grow up with these technologies, some scramble to catch up with the online norms of their teens [29, 140] and to decide on appropriate parenting strategies for their teens' online activity. Parents who look to the popular press, blogs, and child protection software companies for advice will find endorsements for parental monitoring and internet restrictions [119, 55, 118, 129], whereas peer-reviewed research literature cautions against privacy-invasive monitoring [46, 83, 89, 91, 99, 132, 133, 135, 140]. Nonetheless, most parents have experimented with monitoring or restricting their teens' online activities [9].

In this chapter, we present the results of two studies in which we investigated digital parenting strategies designed to mitigate teens' exposure to risky situations online. We focused on experts' and parents' perceptions of how effective these strategies are at reducing risk, and we examined whether parents and teens view these strategies as acceptable to teens.

In the first study, we interviewed 16 experts in fields relating to teen online behavior, online security, online privacy, cybercrime, and monitoring software. We asked these experts for their thoughts on effective and ineffective digital parenting strategies, and from these interviews, we produced a set of seven categories of strategies. Some of these clinical perspectives are not academically published, but are widely disseminated through seminars, popular media, or consumer products. Thus, the collection of expertise presented here contributes beyond what is published in the scientific literature.

In the second study, we surveyed parents and teenagers about the seven categories of strategies established by our expert interviews. We asked participants to rate the effectiveness and acceptability to teens of each strategy. We additionally asked parents for examples of strategies their families have used.

We find that among these seven strategies, some were perceived more positively than others. Feedback from experts showed that monitoring inspired strong opinions both for and against, whereas strategies that relied on open communication of expectations between parents and children received support from all of our expert participants. Survey responses from parents and teens tended to reflect expert opinions of effectiveness, and parents' descriptions of their own strategies echoed sentiments voiced by our experts. Of our seven strategies, education and discussion were viewed in highest esteem by all of our populations. Monitoring, of both the "over the shoulder"

and software-enabled varieties, posed privacy, trust, and logistical challenges that undermined its effectiveness.

Further, we contribute distinctions between parenting strategies under the same umbrella. Monitoring and communication strategies are often grouped in other literature. In contrast, our work suggests that experts, parents, and teens see differences between the two types of monitoring and three types of communication described in this paper. We emphasize that specifying these more narrowly-defined categories allows for a more nuanced understanding of online safety outcomes in families who rely on them. Additionally, we suggested that inactive parenting be studied alongside active parenting strategies, as the participants in our studies indicated that it is a common practice. Recognizing parental complacency alongside other strategies would allow us to understand what safety risks children may be exposed to when a parent is not engaged in the child's online life.

In later chapters, we examine some of the parenting strategies categorized here in more depth. Explicitly, we will examine rules and limits through software monitoring and discussion through an experiment in which families were assigned to use a parental control software (rules/limits, software monitoring) or an online behavior contract (rules/limits, discussion), which were chosen because of the differing professional and parent and teen responses to the strategies of software monitoring and discussion, as addressed in this chapter.

3.1 Background and Related Work

Most teenagers are using the internet daily [65]. Based on almost a decade of research and interviews, boyd writes that daily internet use is the new norm because teens are prevented from gathering in public spaces [16]. As a result, the internet has become their connection to friends, entertainment, and the larger world.

Teens care about the privacy of their digital interactions. In a wide-ranging literature review, Marwick et al. argue that it is important to study teen privacy in the context of technology [81]. Further work demonstrates the strategies by which teens are preserving their online privacy from general audiences. A Pew survey shows that teens are taking control of their online privacy. For example, 74% of teens surveyed had limited their online audiences by deleting someone from their social media friend list [77]. Marwick and boyd interviewed 166 teenagers, and note how teens are talking in coded language, using slang, abbreviations, and allusions to communicate their private thoughts to friends in plain sight on public accounts [80].

3.1.1 Encouragement of Parental Monitoring

Parents must process norms of the online world teens are creating, but at the same time, parents may encounter many public calls to monitor or restrict kids' internet access. One parental control software provider writes, "remember, it's not spying, it's parenting" [119]. The Chief Product Officer of another encourages parents to normalize potentially privacy-invasive practices: "Set up ground rules as a family before you turn them loose. If you do that when they're small, you don't argue with a 16-year-old about privacy. It will just be a part of your family at that point" [55]. And a parenting and child development expert suggests parents interpret child dissatisfaction as a sign of success: "[Teens] will tell you you're ruining their lives... and you will high-five your parenting partner" [55].

Other popular press articles discuss the use of monitoring with more nuance, but they still often suggest parents employ it. One article quotes experts who question whether monitoring software alone is sufficient to keep kids safe online, and argue that communication must underscore any parent's approach, but add that restricting teens' activities will be a more successful way to

control kids' online behavior [118]. Another author establishes a dichotomy of acceptable versus unacceptable use cases for digitally monitoring a child's location using their smartphone, concluding that monitoring for surveillance can be harmful but that monitoring for "safety and verification purposes" is okay [129]. How a parent determines whether they fall under one umbrella or another is left to introspection.

3.1.2 Parenting, in Practice

All of this attention to monitoring children is having an effect, as parents do report monitoring their children's online behavior. According to a Pew survey conducted in 2014 and 2015 of 1,060 parents of teenagers, most parents are monitoring in some form: 61% have checked which websites their teen visits, and 60% have checked their teen's social media profile. Almost half, 48%, have looked through teens' phone calls or messages. And 39% have used parental controls. Parents are also restricting their teens: 65% have taken away a cell phone or internet privileges as a punishment, and 55% have time limits on use [9].

In the same study, 40% of parents frequently discuss what is appropriate to share online, 39% frequently discuss what is appropriate to view online, and 36% frequently discuss what online behavior towards others is appropriate. Notably, 56% of those parents reported frequently discussing appropriate behavior offline. This gap between frequency of discussing online and offline behavior suggests parents are struggling to find the most effective message for online behavior [9].

3.1.3 The Case Against Monitoring

Though supported by some popular press and the software companies themselves, parental monitoring has been heavily scrutinized by previous academic work. Mathiesen argues against parental monitoring from an ethical standpoint in a literature review, asserting that though monitoring can be helpful in some cases to ensure teens' online safety, they have a greater right to privacy that is more important than monitoring in most cases. Instead, she supports communication and negotiation between parents and children: "Parents and children can engage in democratic negotiation of mutual rights, trust and responsibilities with regard to using the Internet" [83].

Newell, Metoyer, and Moore suggest in another literature review that monitoring likely furthers the distrust between parents and teens that it intends to address. They cite work showing that children resist parental monitoring by developing countermeasures, and that children who are subject to environments with parental monitoring see the same incidence of negative outcomes as those whose parents are completely uninvolved [91]. They write:

> Covert monitoring by parents is first perceived as non-engagement by the child. Thus, if successful and never disclosed to the child, all of the risks of parental non-involvement are present. If covert monitoring is discovered, many of these adolescents will take counter measures (keeping two diaries, secret email accounts, etc.) and resist or defeat parental surveillance. ...Moreover, there is now the issue of trust that must be considered by the child—discovered covert monitoring will likely undermine the practice of two-way information sharing.

In an interview with 16 parents of teens, Yardi and Bruckman also caution that teens' privacy is often sacrificed for monitoring, and that adults often do not understand teens' online behavior norms well enough to create appropriate rules [140].

A review of apps designed for teen online safety found a "staggering imbalance that favored parental control over teen self-regulation. This imbalance, in part, may be due to well-intentioned

yet fear-based parenting strategies aimed at keeping teens safe online" [130]. A literature survey by Peters et al. about fear appeals concludes that communication relying on threats or fear do not reduce risky behavior [98], and another researcher writes, in a meta-analysis of why fear appeals succeed and fail, that people respond to fear appeals by ignoring or denying risks, not addressing the threat [136]. These apps may be well-intentioned, but are unlikely to change teens' responses to online risks without actionable advice and education. The few apps that provided features for teens to take an active role in their own safety offered primarily "reach out" features that connected the teen to their parent; only a handful offered any self-monitoring or impulse control features that allow teens to address risks on their own [130].

Monitoring a child's actions online may not be the most effective way to keep them safe in many families, and in some cases, allowing a child to encounter some safety risks may lead to a better long-term outcome. In a secondary analysis of a Pew survey data set, Jia et al. found that teens are more concerned about their privacy after they have encountered a risky situation online [53]. Teens have also been found to perform more risk-coping behaviors after encountering risky situations, demonstrating that they are learning from past experiences [131], and some researchers suggest that low-risk experiences may benefit teens by providing an opportunity to learn resilience [134].

3.1.4 Miscommunication Within Families

Despite academic concern about parental monitoring, many families may still employ some form of it, which could lead to conflict between parent and child. Parents may not be equipped to handle a teen who strongly resists privacy-invasive strategies. Research shows that parents do not always appreciate that teens consider texting friends and other online behavior to be a private activity [29]. Similarly, parents may distrust and be inclined to restrict or monitor apps like Snapchat. They may assume these apps are only useful for sexting, though one survey of adult Snapchat users shows that most users do not primarily use the app for such [105].

A recent diary study found that due to a lack of common understanding between parents and teens, parents consistently underestimate the frequency with which teens encounter risky situations online. This communication breakdown exists in part, Wisniewski et al. state, because when teens tell their parents about these risky situations, parents respond by lecturing and punishing [133].

Even if parents think teens deserve some privacy, research shows that they often use parenting strategies that directly contradict those rights when trying to keep their children safe online [89]. For example, an interview study of 12 parent-teen dyads found that technologically inept parents favored restrictions that could result in a strangling of teens' social connections [135]. Conflict results when parents and teens disagree about teens' privacy needs [46, 99], or teens communicate less with their parents [46]. Researchers Livingstone and Bober caution that the most privacy-invasive practices can strongly inhibit the growth of a positive, trusting relationship between parents and teens [71].

Blackwell et al. suggest that parents have limited visibility into teens' device use—they can tell if a teen is using a device at a glance, but not what they are using it for—which obscures the many positive things teens are doing online. As a result, they found that some parents turn to restricting and monitoring because they doubt their child's activities [15].

Research shows that teens and parents are willing to discuss their concerns together when they share a positive relationship [113], but Yardi and Bruckman found that many parents have trouble implementing authoritative practices that are both demanding of and responsive to children [140]. In an interview paper, Wisniewski et al. conclude that technologically literate parents are the most engaged with what their teens are doing online [135]. In a secondary analysis of 588 teen survey responses, the same research group writes that these parents are also the most successful at keeping teens safe and preserving space for their growth [132].

In this chapter, we seek to understand the merits of different parenting strategies through two studies. In study one, we interview 16 experts and ask them to describe parenting strategies and give their expert opinion about the use of those strategies. In study two, we survey 469 parents and teens, and ask them whether they think strategies are effective and acceptable to learn their perceptions of the strategies they are already employing. Our studies were both approved by the Carnegie Mellon University Institutional Review Board.

3.2   Study One

In our first study, we conducted one-hour semi-structured interviews with 16 expert participants, in which we discussed parenting strategies and their effectiveness.

Occupation	No. of Participants
Educators (E)	3
Technology Industry Professionals (I)	2
Child Protection Software Industry Professionals (P)	2
Law Professionals (L)	2
Researchers (R)	6
Law Professional and Researcher (LR)	1

Table 3.1: Occupations of our study participants. In this text, participants are referred to by a letter representing their occupation (in parentheses above) and a number, e.g. 'E2' denotes that the expert is an educator.

3.2.1   Methodology

Expert 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 contemporaneous 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 3.1. 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. We avoided choosing quotes for this paper that would identify any of our experts. Some research suggests that expert participants should not be anonymized

in order to properly attribute credit for their work [22]. 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

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. 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.

Interview 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. After an initial round of coding, we reduced the codebook to 41 codes in 7 categories. We then finished coding the interviews and reached consensus on our codes.

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.

3.2.2 Results

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 strategies were for the average family—these comments may not apply to different family situations, including strained parent-teen relationships. The seven most prominent strategies are discussed below: software monitoring methods, nontechnical monitoring methods, rules and guidelines, fear appeal, education, discussion, and parental complacency. These are shown in Table 3.2.

Software Monitoring Methods

Our experts were divided on the use of parental controls and other software tools. Four experts (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 experts either did not support the use of tools or supported limited use.

Strategy	Strategy description shown to survey participants
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.
Limits	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.
Discussion	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 3.2: Examples of the parenting strategies drawn from our expert intreviews and used in our survey of teens and parents.

The views of experts who supported software monitoring 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, a parent's right to control the child's device use was paramount. P2 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.

That these four experts endorsed monitoring software is not surprising, given that they 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."

Although the above experts agreed that software is necessary, they did not agree on whether parents should be open with their children about using it. P1, who founded a child protection software company, argued not that children should be benefitting from the experience: "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 that parents should use tools for which children would be unwilling participants: "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 experts all voiced more skepticism towards the use of parental control software. 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." R1 cited considerations for the age and maturity of the child, stating "you cannot have parental control with a 17 year old." L2 was okay with parental controls for "really little kids," but was uncomfortable with their use for most children.

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.

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

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 opponents of monitoring held firm for both software-assisted and non-technical methods, some 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."

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."

Limits

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."

However, experts felt rules often lacked the consistency to make them effective or were unrealistic. Educator E2 noted that teens might say, "Well, you can't take away my device 'cause I have to do my homework." E3 says, rules about online behavior are "not going to be effective if you're not acknowledging what kids are actually wanting to do."

Notably, most of the limits that our experts addressed were aimed at physical devices, preventing loss of sleep, and encouraging more offline social time. But our experts 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 experts strongly supported using the fear appeal. Law enforcement professional L1 declared, "it's not a scare factor. It's a truth factor." P1 described the "pale faces" and "freak[ed] out" reactions to his online safety presentations as positive proof of their effectiveness. 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, and agreed that parents should start educating children 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."

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."

Additionally, 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."

Discussion

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.

3.3   Comparison to Digital Parenting Strategy Literature

Much effort has been devoted to researching parental monitoring of children's online activities. Mathieson [83] and Newell et al. [91] argue against the ethics of monitoring children's digital activities, and Wisniewski and her collaborators [130, 132] have investigated many aspects of parental monitoring. In many of these analyses, monitoring is exclusively defined as software-enabled monitoring of children, or technical and nontechnical monitoring methods are commingled. In discussion with our experts, we conclude that although similar, these two types of monitoring elicit different enough reactions as to be categorized separately from one another. In particular, nontechnical monitoring was more widely supported by our experts than software-based monitoring efforts, and seen as applicable to a larger number of family situations.

Hiniker and her collaborators provide a comprehensive look at rules-setting around family technology use, and are able to suggest that both parents and children have difficulty separating themselves from their devices, so contextual rules are particularly difficult to uphold [51]. However, contextual limits on digital activities may be more appealing than complete bans, as these limits ideally allow for the child and the parent to both get what they want some of the time. The limits suggested by the experts that we interviewed would be classified as contextual, in the scheme described in Hiniker et al. [51].

Little work has been done that focuses on the role that communication-based strategies can play in protecting children from online risks. Discussion between parents and children is often included in broader-ranging work, as a type of parental action [9, 35, 76, 132]. However, our experts drew distinction between the types of communication a parent and child might have. From their contributions, we distinguish three separate types of communication, defined by the goals of the communication. The ubiquitous description of parents and children "talking to each other"

obscures potentially meaningful differences between conversations in which the parent is teaching the child about their family's values and appropriate behavior and those in which the child's contributions are weighted more similarly to the parent's. The first, suggested some of our experts, is particularly important for younger children who are still learning appropriate norms, and the second may be particularly useful as part of the process of teens developing resilience to online risks, as researched by Wisniewski et al. [131].

The lack of distinction within communication also obscures another strategy we identified in this work: the use of fear appeals to scare children into appropriate or safe online behavior. Though the idea of fear-based parenting is briefly mentioned in the conclusion of a study of parental control tools [130], current adolescent online privacy research is largely silent on the matter. Notably, some of our experts advocated using fear-based communication with adolescents during the course of their jobs, when they ran seminars about online safety through local high schools. It is important to capture that teens are being exposed to fear appeals, though fear appeals may not be as popular as monitoring or setting limits, because the use of fear appeals may influence teens' online behavior and receptiveness to other parental risk-mitigation strategies. As discussed in the literature review in Section 2, fear appeals are unlikely to reduce a person's risky behavior [98, 136].

We also find, from discussion with our experts, that parental complacency or inaction is an important component of any investigation of parenting strategies. Most of the works cited above make minor mention of parents who are less proactive, or who do not take steps to mitigate their children's exposure to online risks. However, our experts emphasized that complacency was both common, as parents were often unable to prioritize learning about online norms and risks, and a huge misstep for parents.

3.4 Study Two

In our second study, we conducted 5-10 minute surveys with 469 parent and teen participants, in which we asked about the effectiveness and acceptability to teens of the seven categories of parenting strategies identified in study one.

3.4.1 Methodology

Survey Participants and Recruitment

We recruited our teen participants from outside of a public high school in a large American city during October and November of 2016 using a mobile laboratory with a researcher soliciting participants among passers-by. Each participant was compensated $2.00. Data collection was initially done on laptops, but due to technical difficulties and high demand, most respondents used paper surveys.

We recruited our parent participants in two different ways. We used Amazon's Mechanical Turk (AMT) to conduct a survey in September of 2016. The AMT sample was restricted to the United States, but included some non-parent participants, who were excluded from analysis. Respondents were compensated $1.00. We also recruited local parents by partnering with parent-teacher and similar organizations in February of 2017. Through this partnership, we donated $2.00 to the organization for each completed survey in exchange for the organization advertising in their own mailing lists.

We surveyed 225 teens and 244 parents. Parent responses included 138 from AMT (among 319 total responses, with 181 from non-parent adults) and 106 from PTOs (among 131 total surveys). We eliminated 25 PTO responses that appeared to be tests in which no questions were answered

Pop. (N=469)	n	Mean Age	% Female	% Black
Teens	225	15.7	43.6%	56%
MTurk Parents	138	40.4	52.9%	10.9%
Local Parents	106	46.3	81.9%	8.5%
All Parents	244	42.8	65.4%	9.8%

Table 3.3: Demographics. The teens sample included fewer female participants, and more African Americans, than the parent sample.

after the demographic section. The demographics of our participants are shown in Table 3.3. Note that due to demographic and recruitment differences, we do not statistically compare the parent and teen participants.

Survey Structure

Our survey was designed to take between five and ten minutes to complete. Participants were first asked some demographic questions, including age, race, ethnicity, gender, and whether the participant was a parent of a teenager.

Using a five-point scale, participants rated descriptions seven categories of parenting strategies drawn from the expert interviews in the first part of this study. The exact phrasing used to describe these strategies is seen in Table 3.2. Each strategy was rated on two dimensions: how effective each would be at keeping teens safe online, and how acceptable the strategy would be to teens.

Parents recruited locally also provided an example of the most effective parenting strategy they had used with their own teen, and then indicated which of the seven descriptions best described their strategy, and rated its effectiveness and acceptability to teens.

Lastly, participants indicated how much online activity teens hid from parents, and importance of privacy for teens' social media activity. Again, teens answered from their own point of view, and parents were asked about how their teenager would respond.

In addition to these categories of questions, the survey also included a series of questions about online bullying and the trustworthiness of online strangers, which are not discussed here.

Quantitative Analysis of Survey Results

We conducted within-subjects comparisons using a Wilcoxon Signed Rank test. We used this test to evaluate responses about teens' likelihood of friending strangers and ratings of the effectiveness and acceptability of parenting strategies. We measured relationships between variables using Spearman's rank correlation coefficient (Spearman's ρ), to test whether hiding online activity and the importance of teens' online privacy were related to perceptions of effectiveness and acceptability of parenting strategies. We corrected our alpha value for multiple testing using the Bonferroni method, applied per each type of test.

We conducted initial analyses of the data separately for the two parent samples, and found few differences between significant relationships between parents and teens and within parents. Further, we compared the two parent groups to each other and found no significant differences between how either group responded to the survey. We combine the parent groups in our analysis for more statistical power.

Limitations

Our survey study explored teens' and parents' perceptions of the effectiveness of various online parenting strategies. However, we have only anecdotal evidence as to the actual effectiveness of these strategies, which is much more difficult to observe and measure. Perceptions are still a useful metric, as they provide insights into factors that impact whether strategies are adopted by parents and embraced by teens. Future research might seek ways to observe indicators of the effectiveness of these strategies.

We used convenience samples for this study rather than nationally representative samples, drawing teen participants from a single, large high school, and parents from that and other high schools in the same city as well as online. Thus, our teen and parent samples, in addition to not being nationally representative, are not directly comparable. They differ in major demographic factors, with the teen sample being majority African American and male, and the parent sample being majority white and female. In addition the parent sample was partially recruited using Amazon's Mechanical Turk, which may not be broadly generalizable [66], although the quality of data collected from AMT workers has been shown to be relatively high [23]. When compared, the two parent populations were not statistically different from each other on any variable of interest, partially alleviating concerns about generalizability given the different populations from which these samples were drawn.

Future research might address many of these concerns by recruiting pairs of parents and teens from the same households. This would ensure that both groups have roughly the same demographics and share many of the same experiences with different parenting strategies, and would also allow for more direct examination of teens' perceptions of parents' strategies. This initial examination did not warrant such a time-intensive and costly approach in its efforts to generate insights into possible areas of further exploration.

3.4.2   Results

We first present open-ended responses from our local parent participants about the strategies they use in their own families. We then present a statistical analysis of Likert data from the survey responses of both parents and teens.

Strategies used by Local Parents

We asked local parents to describe an effective parenting strategy they had used to keep their teen safe online, categorize it by selecting as many of the seven types of parenting strategies (using descriptions given in Table 3.2) as were applicable (results in Table 3.4), and then rate it for effectiveness and acceptability.

Most parents described their strategy as involving communication between them and their teen (fear appeal, education, discussion). Fewer parents described their strategy as employing limits or monitoring, and software-based monitoring was the most common of these three strategies. Very few participants described their strategy as complacency.

Parents who reported using nontechnical monitoring described knowing their childrens' passwords, checking devices, and explicitly acknowledged their teens' awareness of this monitoring: "They know that they have to give me their phones to look at whenever I ask." One parent even described it as "the only thing that has impact."

Those who used software monitoring often described situations of conflict within their family because of the monitoring. They reported linking their accounts with their teens' accounts, monitoring location, and generally "snooping" on their teens' social media interactions. But one

Strategy	% Yes
Discussion	75.3%
Education	68%
Fear Appeal	62.9%
Software Monitoring	58.8%
Limits	38.1%
Nontechnical Monitoring	22.7%
Complacency	12.4%

Table 3.4: Percent of local parents who reported using each parenting strategy, ranked from highest to lowest. Participants were allowed to choose more than one strategy.

mother described a situation wherein her daughter and husband both lied to her: "My husband had encouraged her to lie since he felt that it was okay for her to stay out and be somewhere she said she wasn't." She discovered the deception because of a location tracking app on her daughter's phone, and confronted her husband and daughter. Another parent reported that their teens always "seem to be able to get around my monitoring," and that it was "difficult to find the right amount of monitoring without coming across as not trusting them."

Parents' limits restricted the child's screen time or places where a device could be used. A few parents also reported that they "don't allow their children on social media sites."

Parents who used fear appeals frequently cited dangers, risks, and consequences. They emphasized talking about impacts before kids used technology—"teaching Sleeping Beauty the dangers of the spinning wheel ahead of time"—and "giving real examples" from the lives of friends, family, and others teens knew in real life.

Education was discussed as best when started young, "before [children] are faced with peer pressure," with lessons about "what is right and what is wrong." Parents looked for "teaching moments" in which they could explain "responsibility and social media literacy."

When describing discussion, parents highlighted asking questions and sharing experiences. They contrasted this with making accusations or questioning each others' motives, which they sought to avoid. They mentioned trust, self-respect, and privacy, and multiple parents described using peers' situations to springboard dialogue about online safety:

> One of my older daughter's [friends] did get involved in an online harassment incident. We talked about it at home and [discussed] why this happened to that girl and [what] she should have done to avoid it.

One parent's response uniquely discussed how parents could provide support if their own child engaged in a dangerous action: "the parent would be there to support the kid (that doesn't mean what the child did is right but rather we will face the consequences together. Unconditional love)."

Parents who described their strategy as complacent often had the most wide-ranging responses. They wondered, "how can parents monitor all that [a teen's internet activity]?" They described refraining from negative commentary: "I don't usually [speak] or comment on anything.... I try not to give out negative comment on their friends' posts." They concluded descriptions of more complex methods with faith in their teens: "Trusting his own judgement while [being] aware that there will be probably some problems, hopefully not serious!" All of the parents who reported being complacent also reported using another parenting strategy.

We analyzed whether parents who reported using each of these strategies rated their experiences with these strategies as more effective or acceptable than the group of parents who did not use that

Rankings of Effectiveness

Teens		Parents	
a	Complacency	a	Discussion
a	Discussion	a	Education
a	Fear Appeal	b	Nontechnical Monitoring
b	Education	bc	Fear Appeal
b	Nontechnical Monitoring	cd	Limits
bc	Limits	d	Software Monitoring
c	Software Monitoring	e	Complacency

(a) Teens' and parents' rankings of the effectiveness of parenting strategies, ranked from most to least. Strategies labeled by the same letter were not ranked significantly differently from one another.

Rankings of Acceptability to Teens

Teens		Parents	
a	Discussion	a	Discussion
a	Education	a	Education
a	Complacency	b	Fear Appeal
a	Fear Appeal	b	Complacency
b	Limits	c	Limits
b	Software Monitoring	c	Software Monitoring
b	Nontechnical Monitoring	c	Nontechnical Monitoring

(b) Teens' and parents' rankings of the acceptability to teens of parenting strategiesi, ranked from most to least. Strategies labeled by the same letter were not ranked significantly differently from one another.

Table 3.5: Parenting strategy rankings by participant population and measure. Strategies are ordered by mean rank. Each strategy is labeled by one or more letters, where strategies labeled with different letters are ranked significantly differently from each other ($p \leq .002$ for all). Panel A represents parents' and teens' rankings of effectiveness, and Panel B represents their rankings of acceptability to teens.

strategy. We found no difference in level of effectiveness or acceptability of their personal strategy between these groups for each of the seven categories.

Effectiveness and Acceptability of Parenting Strategies

In Table 3.5, we compare perceptions by teens and parents of the seven categories of parenting strategies in terms of their effectiveness and acceptability. We also present the distribution of parents' rankings of these strategies in Table 3.6. In general, teens rated strategies as ineffective and unacceptable, so we present the distributions only for parents, who displayed a greater range of rankings.

Teens viewed software monitoring as less effective than all other methods except limits, as seen in Table 3.5a. Additionally, they viewed limits as less effective than fear appeals, discussion, and complacency. In contrast, parents viewed complacency as the least effective strategy. They also viewed education and discussion as more effective than all other strategies. Among the remaining four strategies in the middle, nontechnical monitoring and fear appeals were both viewed as more effective than software monitoring, and nontechnical monitoring was also seen as better than using

Distribution of Parents' Strategy Rankings

Nontechnical Monitoring	Software Monitoring

Limits	Fear Appeal

Education	Discussion

Complacency
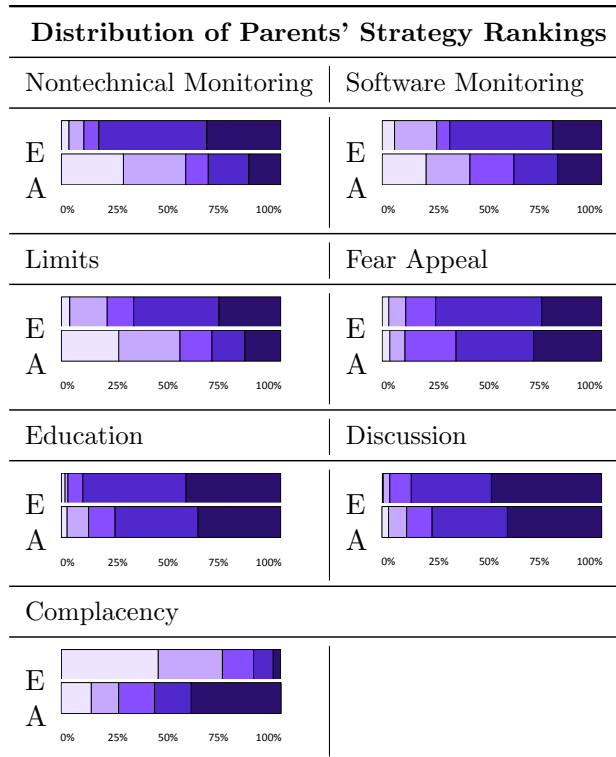
Table 3.6: Parents' rankings of effectiveness (E) and acceptability (A) of parenting strategies aimed at keeping teens safe online, from 1 (light, "ineffective" or "unacceptable") to 5 (dark, "effective" or "acceptable").

limits.

Both teens and parents (Table 3.5b) ranked the more privacy-invasive strategies (nontechnical monitoring, software monitoring, and limits) as less acceptable to teens than the others (fear appeals, education, discussion, and complacency). Parents made some additional distinctions between the less invasive strategies, ranking both fear appeals and complacency as less acceptable than discussion and education.

Demographic Effects on Views of Parenting Strategies

We compared the effects of key demographic characteristics—age, race, and sex—on perceptions by teens and parents of the seven strategies. Among teens, we found no significant effects, but a few differences emerged among parents. Mothers were more likely than fathers to find limits ($U = 4715, p = .003$) and fear appeals ($U = 4832, p = .005$) effective, though they agreed about the acceptability of all parenting strategies. African American parents thought limits ($U = 1570.5, p = .004$) and education ($U = 1606, p = .003$) were more effective than did parents of other races, and younger parents ranked software monitoring as more acceptable than did older parents ($U = 4652.5, p = .001$).

Parenting Strategies and Privacy

We also compared how our participants rated the parenting methods with how they viewed teens' social media privacy. We asked participants to answer both how much of their online activity their teen (or themselves, for teens) hides and how their teen (or themselves) rates the importance of keeping some social media activity private.

Parents' ratings of how much their teens hid their online activity and of the importance of keeping some social media activity private were unrelated to ratings of the seven parenting strategies. In contrast, teens who reported hiding more of their online activity from their parents thought nontechnical monitoring was less effective ($\rho = -.206, p = .002$) and rated their privacy as more important ($\rho = .480, p < .001$).

3.5   Discussion

3.5.1   Parenting Strategy Implications from Varied Perspectives

We identified seven types of digital parenting strategies and asked experts, parents, and teens about their effectiveness and acceptability. Here, we synthesize the perspectives of these three groups to present an overall assessment of the seven strategies and recommendations for further research.

Experts reacted to nontechnical monitoring in a range of ways from total support to total opposition, but many fell somewhere in the middle—though it may be appropriate for younger or immature children, these experts thought this type of monitoring should taper off as the child matured and grew towards adulthood. Our parent respondents also recognized the impact of monitoring, and ranked it as reasonably effective, but they likewise recognized that it would be unacceptable to many teens—something that our teen participants backed up. This strategy thus seems useful if one is mindful of its caveats, and may be best used rarely for many older children.

Software monitoring inspired strong feelings either for or against from our experts, with some calling it the only way to parent effectively, and others decrying its invasiveness. Parents reported challenges using software tools in the home, which was reflected in their rankings of its acceptability to teens. Teens' negative feelings towards software monitoring came out in their low rankings of its effectiveness and acceptability. Overall, software tools seem to need improvements that assuage concerns about needlessly invasive monitoring and address its low acceptability to teens, which currently is the source of some conflict in families that use it.

Limitations on teens' use of digital devices were mostly liked by experts, though parents and teens were more skeptical of their effectiveness and acceptability. Further, both experts and parents described rules primarily aimed at how and when devices were used, rather than rules that encouraged privacy- and security-protective online behavior. Recent research casts doubt on most families' ability to consistently apply rules and limits around device use [51], and combined with the limited scope and low acceptability noted in this paper, this suggests that future work on how to improve family rules about digital devices and online behavior would be valuable.

Though some experts were strongly opposed to using fear appeals as a way to mitigate online risk, others used them as a cornerstone of their digital safety presentations to teens. Over half of our local parent population also reported using fear appeals, most of which seemed to center on real-world examples from their own families or communities. Surprisingly, fear appeals were ranked as effective and fairly acceptable by both teens and parents. All together, this suggests a need to understand how and when stories of risky situations and bad outcomes are appropriate and productive components of digital parenting. As prior work on fear appeals has shown them to often be unsuccessful at reducing risk when not paired with actionable, immediate steps that one can

take to limit risk exposure [136, 54], parents and educators who rely on real-life stories of negative consequences may need direction on how to convert childrens' initial reaction to the stories into positive risk-avoidant online behavior longer-term.

Education and discussion were widely praised by our expert participants and were ranked highly for effectiveness and acceptability to teens by parents and teens. Parents and experts highlighted the need to start online safety education early, before children were exposed to online risks. Discussion was particularly emphasized by our parent participants for its ability to inspire trust between parents and children and to encourage respect for privacy. Given these generally positive feelings from all of our populations, it is worth studying whether adding discussion prompts or educational components to less-agreeable strategies, like software monitoring or limits, might bolster their acceptability while preserving some of the unique benefits of those strategies.

Parental complacency was strikingly unpopular among all of our expert participants and we observed that it was predictably ranked as the least effective strategy by parents. However, open-ended responses from parents who reported letting their children experience the internet on their own shed some light on what a complacent parent looks like in real families. All of these parents also reported employing additional strategies, and the complacency reflected the parent's particular hesitation to act on a specific behavior, with a variety of motivating reasons. Though we recognize that parental non-involvement in part of a child's life and learning is generally not productive, future research might take care to distinguish between the reasons why a parent is not taking action, and address the most concerning reasons first.

3.5.2 Distinctions Among Parenting Strategies

We draw a distinction in this paper between different types of parental monitoring (software monitoring, nontechnical monitoring) and different types of communication between parent and child (fear appeal, education, discussion). In consultation with experts, we determined that these distinctions were necessary for understanding parenting practices and their resultant safety outcomes for the child. For example, few of our experts supported using parental control software to monitor children in most families, citing privacy concerns of the children. However, non-technical monitoring was circumstantially endorsed by a majority of our experts, who understood this style of monitoring to have benefits for younger and less mature children. This difference was supported by our survey of parents and teens, both of whom ranked nontechnical monitoring as a significantly more effective parenting strategy than software monitoring.

Similarly, we specify three modes of communication because experts described differing goals for each mode. Though the use of communication as a whole is supported by most research, including our own, we found that some experts took care to emphasize the weaknesses of fear appeal. Existing literature indicates that fear appeal is largely ineffective at dissuading risky behavior, and so safety outcomes for children whose communication with adults looks like fear appeal may be very different from the safety outcomes for children who engage in equal discussion with adults about online behavior.

These distinctions are a fundamental component of our contribution in this paper. By specifying these more narrowly-defined parenting strategies, as opposed to broader categories of "monitoring" and "communication," our work allows for a more precise understanding of how parenting practices impact long-term online behavior, and safe practices, of children who are exposed to them.

Additionally, we elevate parental complacency to a similar status for analysis as other parenting practices. In past digital parenting and privacy work, inaction on the part of the parent has often been written as simply ineffective. Though our results do not dispute that inactive parenting is perceived as generally ineffective, we recognize that parental complacency is common in many

households, and coexists with other parenting strategies. Therefore, we recommend that it be studied alongside these other strategies to understand what impacts inaction has on the long-term safety outcomes of these families, and what role, if any, complacency can play in family practices.

In the remaining chapters, we discuss the methods and results from two studies whose goals were to examine the categories of parenting strategies named here in more detail. We investigate rules and limits through the lens of both software monitoring and discussion. We chose these strategies to investigate due to the strong disagreement about the use of software monitoring among the experts we interviewed, and the strong support experts, parents, and teens had for a discussion strategy.

Chapter 4

Longitudinal Studies of Parenting Interventions: Overview and Methods

We observed substantial disagreement between online safety professionals, parents of teenagers, and teenagers over which parenting strategies were useful, appropriate, necessary, and effective. We designed two studies to examine two major types of parenting strategies: parental control software and online behavior contracts. Each represented categories of strategies identified in Chapter 3—software represents software monitoring and limits, and the contract represents discussion and limits. We observed usability challenges when participants configured their assigned tools and measured tools' effects over time by studying participants' attitudes towards online risks. We additionally used these studies to investigate a specific risk, cyberbullying, and a related concept, "drama," which were concerns noted by participants in past studies.

In this chapter, we discuss the methodology used in our longitudinal studies of parent-teen dyads. These studies were carried out in two parts: the first was an interview study, where all participants were recruited locally around Pittsburgh, PA and interviewed twice on the Carnegie Mellon campus. The second was a survey study, where participants were recruited from around the United States, and completed two sets of online surveys during the course of the study.

4.1 Recruitment

We recruited our interview participant pairs through postings on social media, community mailing lists, and in-person advertising in public spaces. We recruited our survey participant pairs through social media posts, community mailing lists, paid advertisements on social media, paid advertisements on public transportation, and through our university-maintained participant pool. Our recruitment materials advertised a study in which participants were required to install a parental control software on a child's smartphone. Our ads also indicated that parents would have an opportunity to learn about smartphone safety, and was thus designed to appeal to parents who were interested in teen smartphone safety issues.

For both interview and survey participants, the recruitment ad directed interested parents to a webpage with further information about the study and a dedicated email address to contact for more information. When a potential participant emailed that address, one of the researchers responded with directions to fill out a screening survey that collected the individual's contact information and information about their family, including specific information about the child with whom they intended to participate. We screened for participants who had a child, aged 10-18 years old, willing to participate in the study and who owned an Android phone or Apple iPhone. We interviewed or

Bullying Scenario
Jennifer, a high school student, sees a post about herself on social media made by a classmate. The post is making fun of Jennifer, and has a lot of likes and comments from other classmates adding on. Jennifer's classmate has made a similar post about Jennifer almost every day this week, and Jennifer feels hurt by these posts.
Drama Scenario
Michael, a high school student, sees a post about himself on social media made by a friend. The post is making fun of Michael, and he laughed it off, but wishes the friend would not have made the post.   (Added in the survey study only:)   The friend then replied, "Can't you take a joke?" Both Michael and their friend have a few likes on their comments, and people at school talk about the exchange for a few weeks after.

Table 4.1: The scenarios shown to our study participants to represent different types of online interactions between teenagers.

surveyed one child and one parent per family.

We completed longitudinal interviews with 31 parent-child pairs from June through October of 2017. For their participation in the interview study, participant pairs were compensated with up to $190 in Amazon.com credit: $50 each for the first interview, up to $20 each for weekly surveys throughout the month ($5 per survey), and $25 each for the second interview after one month, for a total of up to $85 for each participant and a total of $190 per pair. In December of 2017, we sent an additional follow-up survey to interview participants, for which they were compensated $25 each, parent and child, for completion. We received responses to this follow-up from 26 parents and 27 children.

We completed 92 paired entrance surveys, 66 condition surveys, and 39 paired exit surveys from February through June of 2018. Data collection for this study is ongoing, and by completion of the study, we anticipate having responses from 100 parent-child pairs for both entrance and exit surveys. For their participation in the survey study, participant pairs were compensated with $80 in Amazon.com credit: $20 each for the first survey, and $20 each for the second survey, for a total of up to $40 for each participant and a total of $80 per pair.

4.2 Study Protocols

Participants in both of these studies were asked to answer questions related to three main areas of interest: cyberbullying and drama, online risk experiences of teenagers, and the configuration and setup of parenting tools. All of the materials used to conduct these interviews and surveys are included in appendices C and D. In this section, we outline them briefly.

4.2.1 Cyberbullying and Drama

In order to understand how our participants understood negative online interactions between teenagers, we devised two scenarios, shown in Table 4.1, to represent different types of interactions. We initially based early versions of these scenarios on dynamics described by Marwick and boyd [79]. We tested 48 variations on the same basic scenario—that one teen made a post about another teen on social media—using Amazon's Mechanical Turk. Analyzing over 900 responses, we

Statement
I / My child has done this kind of thing in the past
This kind of thing has happened to me / my child in the past (I / My child has been in this person's situation)
This kind of behavior is common
This kind of behavior is appropriate
This is bullying
This is typical teen drama
This sounds like a fun interaction
This reflects poor judgment
This kind of behavior is annoying to others

Table 4.2: These statements were shown to participants when participants were asked to describe a given scenario in both the interview and survey studies. In both studies, participants were able to select multiple statements. Additionally, participants were given a write-in "other" response choice.

selected the two scenarios represented in this study because they received the highest percentage of respondents calling them bullying and drama, respectively. After identifying these two scenarios, we further modified them to ensure they were gender neutral. Prior to the survey study, we added the following sentence to the drama scenario in order to better represent drama as it was discussed by our interview participants:

> The friend then replied, "Can't you take a joke?" Both (name) and their friend have a few likes on their comments, and people at school talk about the exchange for a few weeks after.

Participants in our interview and survey studies responded to these scenarios using the statements shown in Table 4.2. They were allowed to choose as many statements as they thought were relevant.

4.2.2 Risky Online Behavior

We asked our participants to respond to a series of Likert-scale questions about a set of predetermined risky online behaviors. The questions and risky behaviors are shown in Table 4.3. We refer to the concepts represented in the questions (severity, likelihood, child's ability to protect themselves, and parent's ability to protect the child) as *attributes* throughout this study.

Based on in-depth feedback from interview participants, we were able to identify sources of possible confusion and nuanced interpretations that called for risky behaviors used for the interviews to be split into separate, more specific prompts. For example, we revised three risks related to accessing types of online content (adult, drug and alcohol, and self-harm) into six so that intentional and unintentional access of these content types were clearly delineated. We also added the risk of encountering online advertisements to create a baseline risk that would be high likelihood and low severity and added pronouns to the risk statements to indicate the role of the child in each risky behavior.

Our Likert scales were labeled only by their endpoints, which ranged from "Not at all [X]" (1) to "Extremely [X]" (5), varying by attribute.

Question
How bad would it be if you experienced the following?
How likely are you to experience each of the following?
How confident are you that you would be able to prevent each of the following?
How confident are you that your parent would be able to protect you from each of the following?

Interview Risk Statements	Survey Risk Statements
Bullying another person online	I bully another person online
Being bullied online by another person	I am bullied online by another person
Visiting sites with sexual or other adult content	
	I come across sites with sexual or other adult content
	I seek out sites with sexual or other adult content
Visiting sites that urge you to use drugs or alcohol	
	I come across online content that encourages the use of drugs or alcohol
	I seek out online content that encourages the use of drugs or alcohol
Visiting websites that urge you to harm yourself	
	I come across websites that urge me to harm myself
	I seek out websites that urge me to harm myself
Illegally downloading copyrighted material, like music	I illegally download copyrighted material, like music
Getting a virus on your phone, tablet, or computer	I get a virus on my phone, tablet, or computer
Texting or talking on the phone while driving	I text on my phone while driving
	I spend too much time using my phone, laptop, or other digital device
Not getting enough sleep because of spending too much time online	I do not get enough sleep because of spending too much time online
Doing poorly in school because of spending too much time online	I do poorly in school because of spending too much time online
Having trouble with friends or family because of spending too much time online	I have trouble with friends or family because of spending too much time online
Being contacted by a stranger	I am contacted by a stranger online
Being abducted by a stranger you met online	I am kidnapped by a stranger I met online
	I am shown an online advertisement

Table 4.3: The phrasing of the Likert questions shown to child participants. Parent participants saw the same questions and risky behaviors, with nouns and pronouns adjusted so that the questions asked about the parent's child.
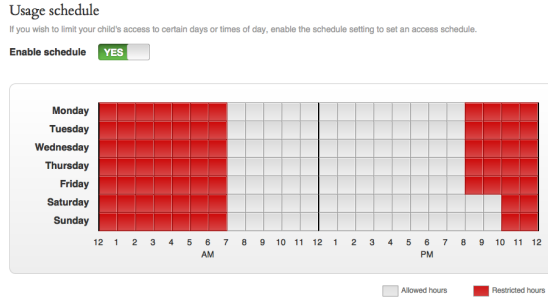
Figure 4.1: A screenshot from Qustodio, displaying a schedule used to limit what time of day a child can use their phone to access the internet. A red block indicates that internet connections are disabled during that hour; grey indicates that internet connections are enabled. Parents may set access hours differently for each day of the week.

4.2.3 Configuring Parenting Tools

The final entrance task for both interview and survey studies was for participants to configure an assigned parenting tool (software or contract), or to discuss the family's household rules in the control condition. Interview participants were provided verbal instructions and directed to think aloud in the lab, but were not asked a specific set of questions during the process. Survey participants could not be observed by the interviewers, and as a proxy, they were prompted with questions about the length of time they spent on this stage of the study, how easy or difficult they found their assigned task, and asked to write a few sentences describing the process.

4.2.4 Follow-Up Survey

Interview participants were offered an optional follow-up survey about three months, on average, from the completion of their final interview. This survey repeated the questions described in section 4.2.2, above. Note that this data has not been analyzed for this thesis.

4.3 Study Procedure

4.3.1 Interview Study Procedure

We conducted our paired interviews with two researchers. We began each interview by obtaining consent from the parent and assent from the minor. Participant pairs were then separated for the first hour of the study, and one researcher interviewed the parent while another interviewed the child in a separate room. Following the individual interview, each participant completed an individual survey.

After both parent and child had completed the survey, the researchers rejoined the participants for the second hour of the study session. In this part of the study, participants were directed to conduct one of three activities, chosen randomly in advance.

Qustodio In the first condition, participants installed a parental control software, Qustodio,[1] on the child's smartphone and configured the tool on a lab computer (Figure 4.1). This software was chosen because it was named a 2017 Editor's Choice parental control and monitoring software by

---

[1]https://www.qustodio.com/en/
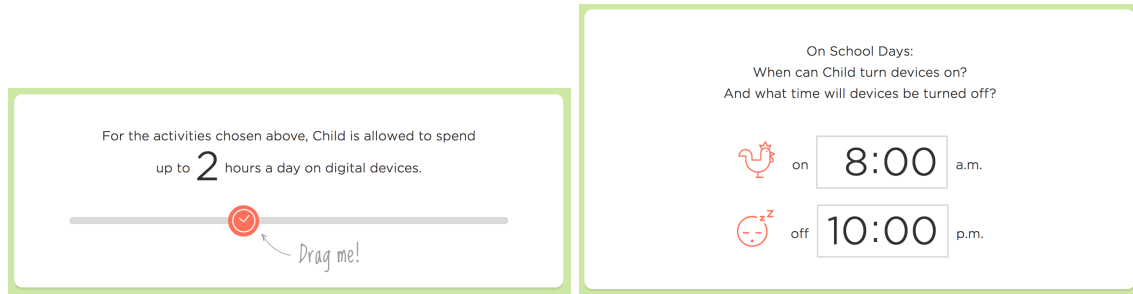
Figure 4.2: Screenshots from The Smart Talk, an online behavior contract maintained by the National PTA and LifeLock. These images show two rule prompts taken from the contract's section on screen time. In the top image, a user can drag the clock icon left or right to decrease or increase the amount of screen time a child is allowed each day. In the second image, a user can type a morning and evening time to govern phone use.

PC Magazine[2] and it worked on both Android and iOS platforms. Qustodio seemed to offer typical parental control features such as content filtering, time scheduling, and location tracking, which are also provided by competitors Kaspersky Safe Kids and Symantic Norton Family.

Qustodio offered seven pages of settings to families. In order, they were web browsing rules, time usage limits, application rules, social monitoring (Facebook only), calls and SMS (Android only), location, and panic button (Android only). Most families took around 20 minutes to configure Qustodio. Installing Qustodio required an app to be installed on the child's device and the settings above configured on a browser by the parent. Qustodio offered both a free and an enhanced paid version of the software, which cost $54.95 or more per year. We purchased a one-year subscription at the $54.95 price point for each of the participants in our studies.

The Smart Talk In the second condition, participants set up an online behavior contract from the website The Smart Talk,[3] on a lab computer (Figure 4.2). This contract required users to set expectations about how the child could use their smartphone, including when the phone could be used, what types of apps the child could or could not install, and how the family would address various types of decisions about phone use that could come up.

The Smart Talk offered 41 prompts to parents and children in six categories, which were as follows: safety & privacy, screen time, social media & respect, apps & downloads, texting & calling, and an extra credit section with miscellaneous questions that did not fit in the first five categories. Similarly to Qustodio, most families took around 20 minutes to complete the contract. The Smart Talk was a free resource that required families to fill out a web form in a browser.

Control Condition In the control condition, participants were prompted to discuss with each other their family's rules about smartphone use. We asked follow-up questions about their rules when appropriate, and we additionally prompted some families about the role of trust in their household when the participants alluded to the concept.

We had 10 participant pairs in the contract condition, 11 pairs in the software condition, and 10 pairs in the control condition. We had an additional pair in the software condition because one of our families had already been using Qustodio prior to beginning our study. Additionally, we added

---

[2]https://www.pcmag.com/article2/0,2817,2473800,00.asp

[3]https://thesmarttalk.org/

the prompt to discuss household rules after the first control condition participants had completed their initial interview, and so we report on only nine paired interviews for control participants.

We then followed up with our participants over the next four weeks. Each week, we sent a short survey to the participants to check in about the child's phone use, and for participants who were given the parental control software, we additionally captured their account settings. Following those four weeks, we conducted a final in-person interview with our participants in the lab. In this second interview, we again separated parent and child. Following the individual interview, each participant completed an individual survey.

4.3.2 Survey Study Procedure

We communicated with our survey participants through a study email address. We began the first set of surveys by sending a survey to the parent, with whom we had been in contact through the screening process. Before seeing the survey questions, the parents were asked to give consent for both their and their child's participation in this study.

Following this survey, parents were emailed a link to the child survey and asked to provide this link to their child. The child survey first asked children to assent to the study. Children were also asked to provide their own email address during the survey so that study researchers could contact them directly during the follow-up survey. Children were asked a similar set of questions to those asked of parents, above.

After both parent and child had completed their individual surveys, they were directed to complete a third survey together, wherein they were assigned to a study condition as described above, in Section 4.3.1. This survey presented instructions for completing the condition requirements: installing Qustodio, negotiating a contract with The Smart Talk, or having a discussion between parent and child in the control condition. After completing the condition set-up, participants were asked to describe their experiences.

We followed up with our participants one month after they completed their condition assignment survey. We separately emailed the parent and the child links to a second survey.

4.3.3 Bullying and Drama Scenarios

Interview participants were randomly shown one of the scenarios (Table 4.1) on paper. The gender of the character in the scenario was matched with the gender of the child in each family, and for cases where the child identified as nonbinary, families were asked which gender they would prefer for the scenario. They were asked to read it and respond by checking statements on a printed response sheet which they thought best described the scenario (Table 4.2). The interviewer and the participant then discussed why the participant selected the statements that they had chosen. Following this, these participants were shown the second scenario, and asked to read it and respond through discussion with the interviewer. The participants were then asked to compare the two scenarios, and then to define cyberbullying and drama.

Survey participants were shown a randomly-selected scenario as part of an online survey, and asked to read and respond to it by checking statements that they thought best described the scenario. Again, the gender of the character in the scenario was matched with the gender of the child in each family. The participant was then shown the second scenario and asked to repeat this procedure, checking statements they thought described the scenario from the same set of responses. To further clarify that the scenarios were separate, different subject names were used in each: Jennifer and Jessica or Michael and Matthew. Following both scenarios, survey participants were asked to define cyberbullying and drama.

Task	Average Length, in Minutes
Entrance Survey, Parent	28
Entrance Survey, Child	22
Condition Assignment Survey	17
Self-Reported Time to Install Qustodio	16
Self-Reported Time to Negotiate The Smart Talk	23
Self-Reported Time to Discuss Household Rules (Control)	19
Exit Survey, Parent	16
Exit Survey, Child	14

Table 4.4: Time required by survey study participants to complete components of the study procedure. Lengths for condition assignment tasks, such as configuring the parental control software or the contract or having the control condition discussion, are based on self-reported data. All other average task lengths are based on data recorded by the survey platform.

4.3.4 Observed Length of Study Tasks

Our entire interview process took, on average, less than the two hours planned for each entrance interview and less than the one hour planned for each exit interview.

Table 4.4 shows the average time survey study participants took to complete study tasks. We calculated survey completion times using data measured by the Qualtrics survey platform, excluding any measurements above 10 hours in order to avoid outliers severely biasing the average completion time. We calculated condition configuration tasks based on participants' self-reported estimates of how long they took to complete the activity. Each task took between 15 and 30 minutes to complete, on average.

4.4 Demographics

4.4.1 A Note on Dropout Rates

The participants described below constitute those from whom we received responses prior to the writing of this thesis. However, we recruited more potential participants than actually participated in our study. Many more people clicked on our advertisements or sent us email inquiries than actually completed the screening survey. Of those who completed the screening survey, approximately 65% completed the entrance interview or survey. All of our interview participants who completed the entrance interview also completed the exit interview. The survey study is ongoing, but it appears that most people who completed the entrance survey, and almost everyone who completed the condition survey, also complete the exit survey.

4.4.2 Interview Participant Demographics

All of our interview participant pairs live in the United States. Of our 31 parents, 27 were female and 4 were male, and 27 were white and 4 were nonwhite or preferred not to answer. The average age of parents in our study was 46 years old, and ranged from 38 to 56. Parent demographics are detailed in Table 4.5. Of our 31 teen participants, 16 were female, 13 were male, and 2 identified as a gender other than male or female. The average age of children in our study was 14 years old, the youngest child was 10, and the oldest child was 18. The most common age for child participants

Parent Demographic Category	#
Female	87.1%
Male	12.9%
White	87.1%
Black	6.5%
Asian	3.2%
No Answer	3.2%
Married	87.1%
Divorced	12.9%
Graduate Degree	64.5%
Bachelor's Degree	29.0%
Associate's Degree	3.2%
Some College	3.2%
Income $200,000 or more	29.0%
$150,000 - $199,999	16.1%
$100,000 - $149,999	25.8%
$75,000 - $99,999	16.1%
$50,000 - $74,999	0%
$35,000 - $49,999	3.2%
$20,000 - $34,999	3.2%
No Answer	6.5%
Mean Age	46.3

Table 4.5: Demographic information about parents in our interview study.

was 12, and we had nine participants of that age. Most (28) of our child participants owned an Apple iPhone; the other 3 children owned an Android smartphone. Children's demographics are detailed in Table 4.6.

4.4.3 Survey Participant Demographics

All of our 92 survey participant pairs live in the United States. Of our parents, 89% were female and 75% were white. The average age of parents in our study was 41 years old. Parent demographics are detailed in Table 4.7. Of our teen participants, 53.2% were female. The average age of children in our study was about 13 years old, the youngest child was 10, and the oldest child was 18. The most common age for child participants was 12. Most (59.5%) of our child participants owned an Apple iPhone; the other children owned an Android smartphone. Children's demographics are detailed in Table 4.8.

4.5 Analysis

Below, we present the analyses used in further chapters in this thesis. We first discuss our analysis of bullying and drama scenarios, the results of which are discussed in detail in Chapter 5. We then present the analyses used for Chapter 6, on online risk perceptions. Finally, we present our analysis

Child Demographic Category	#
Female	51.6%
Male	41.9%
Other	6.5%
Apple iPhone	90.3%
Android Phone	9.7%
Public School Student	64.5%
Private School Student	22.6%
Charter School Student	6.5%
No Answer	6.5%
School Size < 500 Students	48.4%
501 - 1000	29%
1001 - 1500	12.9%
> 1501	16.1%
No Answer	6.5%
Mean Age	13.6
Max	18
Min	10
Mode	12

Table 4.6: Demographic information about children in our interview study.

of the usability of the software and behavior contracts, which is used in Chapter 7. Note that there are some questions in the entrance and exit surveys that are not discussed in this thesis.

4.5.1 Bullying and Drama Analysis

Qualitative Analysis

We asked participants to describe both cyberbullying and online drama in their own words. We coded these free responses, using the codes defined in Table 4.9, where the "target" denotes the person on the receiving end of an online comment or post, and the "instigator" denotes the person who made the initial comment or post. These codes were created iteratively, starting with the three key components of bullying as defined by Olweus [95]: intention to cause harm, where there is an imbalance of social power, that is often repeated over time.

Two coders iteratively reliability-coded 30% of the data. Coders resolved their codes after two or three parent-child pairs of interview transcripts, and revised the codebook as needed. After reliably reaching over 90% agreement, the remaining data were single-coded and reviewed by both coders.

For this analysis, we combined both interview and survey data into the same model. We recognized that study type was a factor in code usage both due to different lengths of response in surveys versus interviews and due to population differences between the two studies, and so we included study type as both a main effect and interacted with our other variables in the model. We do so in order to gain more power for our analysis. Our model was based on the 14 codes defined in Table 4.9.

Quantitative Analysis

For our analysis of qualitatively coded text, we used separate generalized linear mixed models for our interview and survey studies, with family ID as a random effect and participant type (parent or child), code, and whether the participant was describing bullying or drama as fixed effects.

Codes was represented in our data set with a value of '0' if a person's response had never been tagged with the code, and '1' if a person's response had ever been tagged with the code. We chose not to analyze the number of times a participant's response had been tagged with the code in order to minimize the differences in length of responses between participants in the interview and survey studies. We examined significant interactions using post-hoc pairwise T-tests with the Holm-Bonferroni correction.

4.5.2 Risky Behavior Analysis

Qualitative Analysis

We qualitatively coded all interview transcripts and open-response survey data. Our final codebook contained 32 codes in two broad categories, excerpted in Table 4.10. The two categories were "Risks," which encompassed any risky behavior named or described by our participants and which included 21 codes, and "Risk-Avoidance Strategies," which encompassed any strategies that either parent or child used to avoid risky behavior and which included 11 codes.

Two coders iteratively reliability coded 20% of the data, resolving their codes after two or three parent-child pairs of interview transcripts. The codebook was revised as needed. After reliably reaching over 90% agreement, the remaining data were single-coded and reviewed by both coders.

Quantitative Analysis

For our analysis of the Likert responses, we used separate generalized linear mixed models for our interview and survey studies, with family ID as a random effect and participant type (parent or child), study condition (software, contract, control), time (entrance or exit), risk, attribute, parent's gender, and child's gender as fixed effects. The R *lmer* implementation, by default, depends on Restricted Maximum Likelihood Estimation by default to perform fitting. Significant interactions that emerged were interpreted with the aid of simple effects tests and post-hoc pairwise T-tests with the Holm-Bonferroni correction to reveal their underlying patterns.

We split our analysis of Likert questions about online safety risks questions for both the interview and survey studies into two parts: (1) a generalized linear mixed model representing the entire data set, both entrance and exit responses, which did not include any interactions with study condition, and (2) a generalized linear mixed model representing just the exit survey data, which did include interactions with study condition. We made this choice in order to preserve three-way interactions as our highest order of interactions, and minimize the chance of misinterpreting complex results. In order to interpret the second model, we compared the entrance responses between participants in each study condition to see whether the conditions were truly randomized. In both studies, there was not a significant difference between these populations ($p > 0.05$), and for the survey study, all conditions were fully independent ($p > 0.3$). However, for the interview study, we note that the software condition participants were not fully independent from the control population ($p = 0.116$). This may be a result of the small sample size in each condition ($n = 10$ or 11).

The first and second model both used family id as a random effect. The first model held time (entrance or exit), condition, participant type (parent or child), child's gender, parent's gender,

risk, and attribute as fixed effects. The second model held all of the same fixed effects except for time.

We note that the attributes we refer to in Chapter 6, which are determined by the question to which a participant was responding when evaluating risks (see Table 4.3), were all significantly different from one another in each model ($p < 0.001$ for all). Thus we have established four separate measures of risk, and in all analyses below, attribute plays an integral role. We do not evaluate risks without attributes because it is meaningless to take a mean of a given risk across all attributes under which it was evaluated. We also present analyses which include only attribute, and not individual risks, to show trends across all risks.

4.5.3 Usability Analysis

We single-coded recordings of our interview participants setting up the software or contract, or discussing household rules, in the lab. Before coding began, we examined the software and contract interfaces and built a preliminary codebook around the features offered by each tool. A research assistant then coded these interviews iteratively with the goal of identifying themes related to the participants' experience with their tool or discussion. The research assistant also noted conversational patterns, such as disagreements between parent and child or places where the participants asked the interviewer a question, to aid in identifying usability issues. After each interview, the research assistant wrote a summary of the family's experience and noted ongoing and emerging themes. The primary researcher and research assistant met weekly and discussed the findings.

4.5.4 Future Work

The data presented in this thesis are part of a larger, ongoing analysis, as of the time of writing. In future work, we will examine the collected data that are not represented in the body of this document. We are also collecting additional survey responses, and anticipate that all analyses of the survey study may be subject to change or expansion with the inclusion of the further survey responses.

In particular, we hope to examine effects of a child's age on risk perceptions once we complete collection of our larger sample. Based on feedback from teens, parents, and online safety professionals in Chapters 2 and 3, many families think that a child's age should influence parenting strategy. In this view, an older or more mature child should be allowed more freedom to choose their own behavior, and younger or less mature children should be more constrained. We might expect to see that ratings of severity of certain risks are lower for older children than younger, or that parents have higher confidence in older children's ability to prevent risks. We will investigate this in the full data set.

Additionally, we intend to investigate how survey study participants configured their software and contracts once the full sample has been collected. We plan to report which settings were changed from the defaults and what percent of the participants chose each setting. We hope to gain an understanding of how these tools are generally used by families and which settings were most and least commonly configured.

We also plan to analyze the remaining questions on the surveys given to both interview and survey study participants. We asked questions about the use of categories of parenting strategies and the frequency of specific parenting behaviors. We would like to examine the responses to these in comparison to evaluations of risk, and see whether certain parenting strategies or behaviors are correlated with certain reactions to online risks.

Parent Demographic Category	#
Female	89.1%
Male	8.7%
Other	1.1%
Decline to Answer	1.1%
White	75.0%
Black	20.7%
Asian	1.1%
Decline to Answer	3.3%
Married	73.9%
Divorced	14.1%
Never Married	8.7%
Living with Partner	7.6%
Separated	5.4%
Widowed	1.1%
Decline to Answer	2.2%
Graduate Degree	35.9%
Bachelor's Degree	29.3%
Associate's Degree	7.6%
Some College	19.6%
High School Degree or Equivalent	7.6%
Income $200,000 or more	6.5%
$150,000 - $199,999	7.6%
$100,000 - $149,999	23.9%
$75,000 - $99,999	14.1%
$50,000 - $74,999	18.5%
$35,000 - $49,999	5.4%
$20,000 - $34,999	20.7%
Less than $20,000	7.6%
Decline to Answer	3.2%
Mean Age	40.8

Table 4.7: Demographic information about parents in our survey study.

Child Demographic Category	#
Female	53.2%
Male	45.6%
Other	1.3%
Apple iPhone	59.5%
Android Phone	40.5%
Public School Student	73.9%
Private School Student	10.9%
Charter School Student	9.8%
Home School Student	3.2%
Other	2.2%
School Size < 500 Students	36.9%
501 - 1000	47.8%
1001 - 1500	7.6%
> 1501	8.7%
Mean Age	12.9
Max	18
Min	10
Mode	12

Table 4.8: Demographic information about children in our survey study.

Code	Definition
Anger	The target of bullying or drama responds by getting angry at the person or people involved
Back-and-Forth	The target of bullying or drama responds by fighting back, beginning a chain of bullying or drama incidents, bickering, or similar
Communication Control	The instigator of bullying or drama uses features of a technology platform to enable their actions, e.g. an anonymous messaging system
Conditional Reaction	The target of bullying or drama's response is specified as determining whether an event is bullying, drama, or something else by the participant
Content	The content of an instigator's online posts determine whether something is bullying or drama, e.g. making appearance-related insults
Nonreaction	The target of bullying or drama responds by not caring about the incident or otherwise not reaction
Exaggeration	The target of bullying or drama responds with an exaggerated or outsized reaction to the incident
Hurt Reaction	The target of bullying or drama feels hurt or harmed by the action
Intent to Hurt	The instigator of bullying or drama intends to cause harm to the target of their actions
Permanence of Content	The potential for online posts to stick around a long time, potentially forever, makes something bullying or drama
Permission	Whether the instigator making a post has permission from the target of the post to share that content, and that makes something bullying or drama
Power Imbalance	The instigator of bullying or drama has more power (e.g. social or physical) than the target of their actions
Repetition	Whether the bullying or drama is a repeated event for the target
Serious Harm	The target of bullying or drama experiences serious negative fallout from these experiences, e.g. self-harm or depression

Table 4.9: The codes used to characterize participants' open-ended responses to questions about online bullying and drama.

Category	Sample Codes	Definition
Risks	Adult Content	The risk is a child's exposure to "adult" or "inappropriate" content, which may include sexual content/nudity, violence, swearing or vulgar language, etc.
	Phishing	The child is targeted by a phishing scam through email, text, phone call, etc.
	Too Much Time Online	The risk is a child spending too much time online, getting sucked in to a device or app, etc. The time online is itself a negative effect.
Risk-Avoidance Strategies	Non-Technical Monitoring	Looking at children's social media accounts and reading their posts and messages to monitor what they are doing online.
	Privacy/Security Settings	Child uses or is encouraged to use privacy/security settings provided by a device or social networking site in order to protect themself from online risks.
	Software Monitoring	Using parental controls and other software tools to monitor what children are doing online.

Table 4.10: Some of the codes used when coding discussions of risky online behaviors in both the interview and survey longitudinal studies.

Chapter 5

Cyberbullying and Drama

5.1 Introduction and Background

One of the risks to teens that we encountered in our discussion with experts in Chapter 3 was cyberbullying. Cyberbullying is a frequent spectre in the news and popular media, featuring in events like the Gamergate controversy over the representation of women in video games[1], television shows like *13 Reasons Why* about a teen girl who committed suicide after being bullied online[2], and public outreach campaigns like the recent Be Best initiative from First Lady Melania Trump[3]. The increasing cultural awareness of cyberbullying as a growing problem without a clear solution was reflected in our own data from experts, parents, and teens alike.

5.1.1 Cyberbullying Literature

Cyberbullying is a concept that has been increasingly examined in the scientific literature. Research on online bullying draws heavily from offline bullying literature, and most definitions are adapted from the Dan Olweus definition of bullying: "A student is being bullied or victimized when he or she is exposed, repeatedly and over time, to negative actions on the part of one or more other students" [95]. This definition has been re-imagined for cyberbullying by Olweus himself [96], and this revision and others are compared in detail in a literature review [58]. Of note is a taxonomy that delineates different forms cyberbullying can take, including those that look very similar to offline forms of bullying, such as exclusion from social groups, as well as forms that are made more feasible by the internet, such as impersonating someone else to make them look bad [128].

Cyberbullying does not yet seem to have a widely-accepted definition, despite this work, as noted in the 2014 review by Kowalski et al. [58]. This seems, in part, a result of the shifting digital landscape. Patchin and Hinduja defined cyberbullying along fairly standard lines established in earlier bullying work, but specified a twist on power imbalances between bullies and their victims in the digital realm: "anyone who can utilize technology in a way that allows them to mistreat others is in a position of power—at least at that moment—relative to the target of the attack [97]. This idea was repeated in more recent work, which suggested that early adopters of technology can weaponize emerging apps against their peers [111].

Other core concepts of bullying have been similarly re-imagined. Slonje et al. noted that repetition historically refers to repeated events across multiple days, but cyberbullying might evoke

---

[1]https://www.npr.org/sections/alltechconsidered/2014/09/24/349835297/-gamergate-controversy-fuels-debate-on-women-and-video-games

[2]https://www.netflix.com/title/80117470

[3]https://www.whitehouse.gov/bebest/

repetition in the way that a single piece of content can be reposted multiple times by many people. Similarly, they described the complicated role of audiences in cyberbullying: audiences can be much larger than those of traditional bullying, thanks to technology, and bystanders may exist at multiple places in the interaction, including with the perpetrator when content is posted, with the victim when content is received, or on their own when content is broadcast on a platform [112].

Cyberbullying interventions also remain an area in need of more study. Cioppa et al. investigated 12 intervention programs aimed at stopping and reducing cyberbullying. They found that most lack scientific backing and pose implementation challenges for schools or organizations that would like to use them. They called for programs that are evidenced-based and that have sustained, integrated components which encourage the maintenance of good online behavior rather than drop-in one-off interventions [32].

It is important that researchers continue to identify and fill the gaps in cyberbullying research because cyberbullying can have significant negative effects on people. Aboujaoude et al. reviewed scholarly work on the effects of cyberbullying and found a number of concerns: a large minority of minors experience cyberbullying (20%–40%), girls and sexual minorities are at higher risk of being victims of cyberbullying, and there is a "well-established" link between being the victim of cyberbullying and feeling suicidal [5]. Another review from the same year found similar results: about 20% of minors were involved in cyberbullying, and that sexual minorities were more likely to be victimized [144]. Both of these reviews highlight that cyberbullying, much like traditional bullying, has a disproportionate impact on already-vulnerable populations (minors, women, sexual minorities).

5.1.2 Research on Drama and Related Concepts

Marwick and boyd find that, for teens, not all online aggression reaches the standard of bullying [79]. Instead, teens seem to view a lot of negative online interactions under the hazier term "drama," borrowed from the earlier work of Kathleen Allen [6]. Marwick and boyd write:

> 'Drama' allows for a kind of blurriness and liminality in teen practice that is not afforded by the terms 'bullying,' 'relational aggresion,' or 'gossip.' Drama incorporates a spectrum of seriousness, which includes joking, 'talking trash,' and serious anger.

They describe results from an ethnographic study of teens aged 13 to 19, taking place from 2006–2009 and 2010–2011. In interviews, their participants often organically discussed the concept of drama, and separated it from other, similar concepts, as mentioned above. The authors noticed that these teens might describe a situation of repeated, targeted, hurtful remarks as just drama, but that adults might think those interactions are clearly bullying. Indeed, Marwick and boyd quote a teen's story, which focused on a girl tormenting another girl over Facebook and text messages about a boy who had romantically pursued them both, that neatly fits the Olweus definition of bullying despite the teens involved referring to it as just drama [95].

Our research aimed to build on the findings put forth by Marwick and boyd by exploring how parents and teens from the same families understand the terms "bullying" and "drama." If teens do use the term drama where adults use bullying, then teachers, parents, and other mentors might face significant challenges in combating hurtful and negative interactions between teens. In this study, we explore the concepts of drama and cyberbullying with both teens and parents, and we use a combination of pre-written scenarios and open-ended discussion to most thoroughly probe the topics.

Kathleen Allen's work to define drama was a key source for Marwick and boyd's study, discussed above. Allen set out to understand bullying through text messaging in a suburban US high school,

and found that though both students and staff say bullying is not common at their school, they described a concept they called drama and admit it happens regularly. Allen made note of this concept and suggested it could lead to more serious incidents of bullying. She concluded by calling for more study of drama separate from other types of conflict and bullying [6], a space into which the 2014 paper from Marwick and boyd fits.

Allen continued to study drama in further work [7, 8]. She found that "a major issue for adults [teachers and staff at a high school] was making a determination as to whether the situation [between teens] was or was not bullying," a challenge that could negatively impact the adults' ability to help students. Allen additionally surveyed participants, teens, teachers, and staff, at a high school and tested five vignettes about online interactions between teens. Participants were asked to rate these vignettes on a 1–5 scale, according to whether the vignette was an example of bullying. One vignette represented drama; it described a relationship and friendship conflict around one couple, a boyfriend and a girlfriend, and a male and female friend of the girlfriend. She found that the drama vignette was the vignette with the lowest mean on the bullying scale.

In addition to the research by Marwick and boyd, as well as research by Allen, which study drama explicitly as a concept separate from bullying, other researchers have studied aggressive online behavior that may not be bullying.

France et al. conducted an online survey to study instances of "brief" versus "extended" cyber aggression, where they characterized extended cyber aggression as cyberbullying. They hypothesized, based on common definitions of cyberbullying in other literature [56, 61, 141], that perpetrators of extended cyber aggression were distinct from perpetrators of brief cyber aggression [40].

Instead, they found that there are not many differences between these types of perpetrators, and further, that both groups thought there should be offline consequences for aggressive behavior online. They also suggested that brief cyber aggression incidents may be more common than extended incidents—more than one third of participants identified themselves as perpetrators of brief cyber aggression. As a result, much research on cyberbullying, where cyberbullying is defined in part by repetition, may miss important incidents of aggressive online behavior [40].

5.2   Results

We asked parents and teens to share their views about scenarios involving online conflict (See section 4.2.1 for details) in interviews and surveys (section 4.3.3). Responses were coded and analyzed (section 4.5.1). The data presented in this chapter represent combined responses from both the interivew and survey participants, up to 123 families in total.

5.2.1   Bullying and Drama Scenarios

The bullying scenario was almost universally recognized as such, but about 24.7% of participants also identified it as drama. In contrast, the drama scenario was seen similarly as bullying and drama, with about 39.4% labeling it only as bullying, 22.4% only as drama, and 22.9% as both, suggesting that drama is not a subset of bullying because over a fifth of participants thought this scenario was only an example of drama, not bullying. These results can be seen in Figure 5.1. This pattern of results is reflected in two main effects and an interaction: first, both scenarios were labeled more often as bullying than as drama in the interviews ($p = 0.007$) and surveys ($p < 0.001$). Second, the bullying scenario was labeled as both bullying and drama more often than its drama counterpart, a finding that was significant for the surveys ($p = 0.002$) but not the interviews ($p = 0.172$). And third, an interaction reflected the larger gap in labeling the bullying scenario as bullying versus drama as compared to a smaller gap when labeling the drama scenario
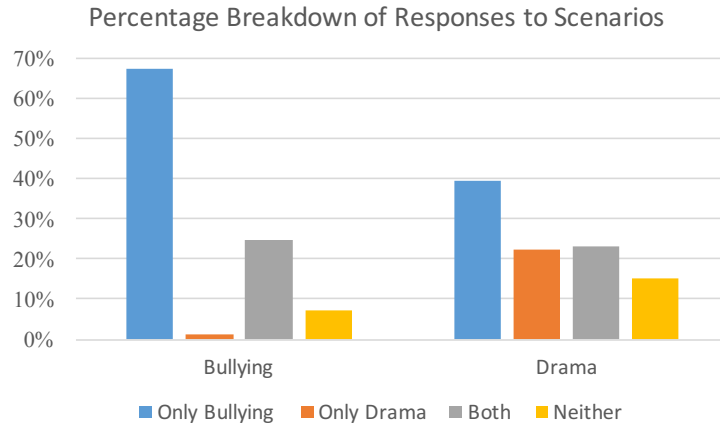
Figure 5.1: A chart displaying the percentage of responses to each scenario where the respondent chose only the statement "This is bullying," only the statement "This is typical teen drama," both statements, or neither statement, by bullying and drama scenario (grouped along the x-axis). Each cluster of bars represents 100% of the responses to the bullying and drama scenarios. In total, we received 402 responses from 123 pairs of interview and survey participants.

as such in surveys ($p = 0.017$), which did not reach significance for interview data ($p = 0.051$). The smaller sample in our interview data resulted in lower power for those analyses, but the pattern of results appear similar to that found in the survey data.

There was no effect of participant type on how scenarios were described ($p = 0.900$ interview, $p = 0.386$ survey), which suggests that parents and children did not use the label "drama" in different ways, contrary to our initial expectations based on prior literature. There was also no effect of the gender of the scenario subject (again, matched to the child participant's gender) on how the scenarios were described ($p = 0.974$ interview, $p = 0.698$ survey). The non-gendered nature of our scenarios is a possible reason for not finding the gender effects that others have found [8, 79]; a strength of this is that boys might see drama just as easily in their own conflicts, but that may be lost when including context from anecdotal scenarios, such as which actions a boyfriend versus a girlfriend takes during a breakup.

In fact, our participants expressed gendered understandings of drama, similar to those described in those earlier works on drama. Many parents and children mentioned that drama primarily took place between girls, or emphasized the relative rarity or different nature of "boy drama." One 13-year-old boy described his own, apparently unusual, experience of drama with another boy:

> Girls are like, "Oh, there's boy drama happening!" There's this one kid in my grade... who can be a little bit annoying at times. I mean he's nice and he's my friend but... We were presenting a project... and [he] corrected me in the middle of the presentation... and I was like no you're wrong cause I thought he was wrong. It turns out he was right but whatever. Maybe we were both wrong, I don't remember. But either way he corrected me when we were in the middle of presenting and... I was like, "Don't correct me in the middle, I know I'm right." And then we got into an argument in the middle of presenting and we got a C on our project so.

The sentiments underlying this experience are similar to those a girl might feel following relationship or friend circle drama: the boy felt hurt by his friend's action in the moment, and reacted

66

angrily by fighting back, eventually exaggerating the disagreement into an argument in front of their peers and teacher. These actions and feelings follow exactly from how drama has been previously characterized [6, 7, 8, 79], but the details are "male," or at least not "female," in the eyes of this participant.

5.2.2 Bullying and Drama Open Response Analysis

We used a mixed model logistic regression to compare how our participants talked about bullying and drama as described in section 4.5.1. Of the 14 codes used in our regression model, three were involved in significant interactions: intention to hurt another person, repetition of actions, and communication control. These are discussed below. Analyses identify when any given code is used more or less often to describe drama than to describe bullying.

Bullying: Intent and Repetition

Participants described an instigator wanting to hurt another person as a way to identify bullying more often than to identify drama ($p = 0.022$). For example one mother of a 13-year-old boy describing bullies "do[ing] cruel things" to their targets, and an overall trend of deliberate humiliation, insult, and harassment.

Participants also described bullying as a repeated, ongoing, and constant behavior more often than they described drama as such ($p = 0.006$). One 12-year-old girl explained that bullying means that someone "won't stop" picking on you. Both this repetition and the above-mentioned intention to hurt someone represent two of the core components of bullying defined by Olweus [95].

That these were more strongly associated with descriptions of bullying than descriptions of drama suggests that our participants, parents and children, perceive bullying similarly to how it is defined in the scientific literature, indicating that it is a well-defined and widely understood concept. In our sample, adults and children operate with very similar understandings of bullying, differing primarily over how each group perceived the influence of technology on power structures among peers.

Technology-Mediated Power Imbalances

Our participants described the type of power differential in Olweus' definition, noting social status, population, and reputation as factors that make up bullying.

However, our participants described an additional form of power imbalance between adolescents: an imbalance mediated by technology and the social platforms on which children were interacting (the code "Communication Control" in Table 4.9). We found that child participants in our studies described this concept significantly more often when discussing bullying versus when discussing drama ($p = 0.010$), though we note that the concept was discussed more often in interviews than in surveys ($p < 0.001$ for both parent and child). Parents were not significantly more likely to associate this concept with either bullying or drama ($p = 0.77$).

One might expect that participants thought of anonymous social media platforms as a space where bullies could be more powerful than their peers. Some participants did discuss secret and anonymous behavior, including one 15-year-old girl who explained that because online bullying was not "face to face... [bullies] can come together in a second and... now it's a bunch of people bullying you." In our second interview, this girl shared that she had been bullied during the period of study[4] through the Sarahah app, which she linked to her Snapchat account. She read from the

---

[4]The author of this study confirmed, during the time of interview, that the girl's mother was aware of this bullying.

anonymous messages she received:

> "You're creepy as [expletive] because you legit curse like a demon... Go to church once in a while. Praise God, may the Lord and Savior protect you." Damn. That was really hurtful...
>
> I hated that. It's different if you say it to my face.

In reality, discussions of anonymous platforms like Sarahah made up only about 18.5% of the times the "Communication Control" code was used across both bullying and drama (they were 27.8% of bullying-specific mentions and 0% of drama-specific mentions). Parents mentioned anonymity 60% of the time, and children the other 40% of the time, but the sample is small enough that we will not speculate on trends for a larger population.

Overwhelmingly, the discussions we coded centered on the concept of the interaction not being "face-to-face." Children suggested that bullies were disconnected from their targets; one 14-year-old girl specified that this form of bullying was "cowardly," or in the words of a 13-year-old girl, that these bullies would be too "scared" to do the same thing in person.

The emphasis placed by children on social media or digital devices removing the personal, face-to-face element of interactions suggests to us that some form of power imbalance is created by digital platforms where it might not otherwise exist, even when the bully is posting under their own name.

5.3 Discussion

5.3.1 Parent and Child Perceptions of Drama

Marwick and boyd [79] describe drama as a label that teens apply to define their own narrative of online conflict in their peer communities, and a label that their parents may not understand. Our results do not entirely support this understanding of drama as a concept unknown to parents, and many parents were able to define and differentiate drama from cyberbullying in ways similar to how their children defined and differentiated the two concepts.

There are a couple of probable reasons for the differences in our findings. For one, Marwick and boyd conducted their interviews with participants 6–12 years prior to our own data collection. In that time, the concept of drama may have spread from teenagers to their parents, or become part of a wider cultural dialogue, and so parents in our sample were more aware of it than parents 6–12 years ago may have been. Another possibility is that Marwick and boyd did not interview parents of teenagers in their study, and their conception of what parents of teens were aware of may have been inaccurate. By studying parents and children in the same families, we guarded against the possibility that our parent data reflected concerns about teens that were somehow different from our own sample of teens; by including teens and their own parents we can control for such population problems.

5.3.2 Gendered Perceptions of Drama

Work by Allen [6, 7, 8] and Marwick and boyd [79] has discussed how adults and children may perceive drama as a gendered activity, something that girls engage in but boys largely do not, unless those boys are at the center of girls' romantic dramas. Our studies do not dispute that people perceive drama this way, but they do suggest that people may apply the "drama" label similarly regardless of whether the subject of drama is given a male or female name.

We believe that further study of how gender intersects with drama is worthwhile. If "boy drama" is not identified as readily as "girl drama" by peers and adults, boys might not be able to resolve their conflicts before the conflicts create larger problems, whether that is bullying or the end of a friendship. Likewise, understanding drama as actions typical of girls might ignore drama between girls and girls or girls and boys that does not adhere to gender norms. The goal of studying conflict and drama between children and teens is to find productive paths to addressing it and minimizing harm, and to do so, we must recognize drama in all its forms and be aware of how assumptions might prevent that recognition.

5.3.3 Impact of Technology-Mediated Power Imbalance

Our study found some difference in how children and their parents approach instances of online conflict. Parents and children in our study identify different asymmetries between the instigator of an online conflict and the target. Children describe technology-enabled asymmetries, such as the use of an anonymous messaging app like Sarhahah to send critical, negative messages to someone. Parents did not see this as a distinct attribute of bullying, the way that children did. A similar type of power imbalance has been noted in other research on cyberbullying: power imbalances may be created by technological proficiency with a platform [97, 111, 112].

Our results do not suggest whether this proficiency is at the root of the power imbalance perceived by the children in our study, though we believe that this is a meaningful area for future work. In particular, we see a few possible, potentially overlapping, explanations for this power imbalance: the above-mentioned concern about technological proficiency, the inability for even a technologically-proficient child to respond to anonymous bullying, and the disconnection or depersonalization that results from not being face-to-face with your target.

On the other hand, we did not observe any differences in how parents and children described social and relational asymmetries, such as a more popular child bullying a less popular child. Both of these asymmetries enable an instigator to more easily carry out or get away with their actions, and limit the ability of a target to confront the instigator.

Despite these similarities, responses to these situations may necessarily be different. Though a parent or educator may be able to bring together two children of different social status in a neutral setting to talk through a conflict, that remedy may not be available if the instigator is anonymous. Additionally, if parents or other adults are not aware of or comfortable with the technology they might face obstacles to understanding an online conflict situation. One can imagine a school administrator struggling to help a student who cannot prove the identity of their bully because a message was sent anonymously, or who cannot prove the existence of the bullying because the message was sent through a disappearing-message platform.

Chapter 6

Online Safety Risks

6.1 Introduction and Background

In Chapters 2 and 3, we saw heard from many people who worried about children's online safety. Their concerns ranged across a spectrum of risks, from children consuming mature content online to children being abused by online predators. The perception of online safety risks, and the ability of parenting tools to change that perception, are the focus of this chapter.

6.1.1 Rise in General Internet Use and Addiction Concerns

Smartphone ownership is nearly ubiquitous, allowing young people access to the internet almost anywhere. Pew Research Center reports that 95% of Americans own some type of cellphone and 77% own smartphones, based upon survey data collected in 2016. This percentage has more than doubled since Pew's first survey of smartphone ownership in 2011. The percentage is also higher for younger generations: Pew reports that 100% of survey respondents ages 18-29 own cellphones of some kind and that 92% own smartphones [26].

For many users, smartphones bring great utility. However, 57% of smartphone users surveyed in 2014 and 2015 reported feeling "distracted" by their devices, and 36% reported feelings of frustration. Younger users, in particular, were more likely to report both positive emotions such as gratefulness *and* negative emotions such as anger and distraction [114].

Since the rise of home internet access in the 1990s, some researchers have been concerned that the internet might be distracting, harmful, or potentially even addictive. In 1998, Young [142] developed an eight-item questionnaire for identifying individuals with internet addiction that spotlighted qualities such as irritability when decreasing internet usage and lying about one's amount of internet usage. Similar scales to identify addiction to smartphone use have been tested more recently for adults [67, 60] as well as adolescents [59].

Some researchers have argued that a high level of engagement with the internet and/or with internet-enabled devices such as smartphones does not meet the criteria for clinical addiction [42, 16], and the American Psychiatric Association does not currently recognize internet addiction or smartphone addiction as diagnoses [11]. Regardless, since the early days of the internet, users have reported problems engaging in healthy and safe internet usage, and these challenges have increased with the pervasiveness of internet-capable devices, including smartphones, in the modern world.

6.1.2 Pervasive Adolescent Use of Smartphones

Smartphone usage is particularly pervasive among younger generations, and this increasingly includes adolescents. Among teenagers (ages 13-17) surveyed in 2018 by Pew, 95% reported having access to a smartphone. Almost all (89%) reported going online several times per day or more, and 45% of teens reported using the internet "almost constantly" [10].

As of 2010, Pew Research reported that most children were getting their first cell phone at age 12 or 13, but that younger teens were more likely than older teens to have received a cell phone at an earlier age, suggesting that the average age of first-time phone owners is getting younger [64]. A more recent report from the market research firm Influence Central, published in 2016, found that the average age of first-time smartphone owners was 10.3 years old [4]. This report did not include demographic details for its 500 participants, all of whom were women, and so we cannot say with certainty that 10.3 is the average age of American children receiving their first smartphone, but their findings are consistent with the earlier work from Pew Research.

In her 2014 book, boyd extensively discusses the premise that teens are addicted to spending time online, specifically on social media. She dismisses this idea, suggesting instead that teens respond to restrictions on their ability to physically socialize by digitally socializing with their peers [16]. Her work strongly cautions against pathologizing what she describes as a normal impulse to communicate. However, in the time since boyd's research was conducted, many more children have become smartphone owners, and concerns about ubiquitous phone use raise new questions about what are the risks of excessive internet use and how best for families to address it.

6.1.3 Research on Risks of Teen Smartphone Use

Researchers and parents alike raise concerns about the effects of increased technology and smartphone use on the general health of children and teenagers. Rosen et al. [107] surveyed 1030 parents regarding their own behaviors and those of their children, and found that "for teenagers, nearly every type of technological activity predicted poor health."

Many researchers have also highlighted potential negative effects of excess technology usage on children's and teenagers' sleep. Hale and Guan [43] review 67 studies published between 1999 and 2014 on the association between screen time and sleep outcomes for school-aged children and teenagers. This review shows that, in 90% of studies considered, screen time is adversely associated with sleep outcomes (shortened duration as well as delayed timing). Hale and Guan do note that these studies have some methodological limitations and that causation has not been confirmed, but they still advise that children and teenagers limit their screen time, particularly before and during bedtime hours. In a policy statement in 2016, the American Academy of Pediatrics advised that children should not sleep with devices such as televisions, computers, or smartphones in their bedrooms [49].

Meal time, especially family dinnertime, is often a source of tension between parents and children around technology use. Moser et al. [87] examined attitudes surrounding mobile phone in a survey study and found that attitudes were affected by three main factors. The first of these was participants' own mobile phone use. The second was age: it was less appropriate for children to use phones at the table than for adults to do so. Third was the presence of a child at the table: it was less appropriate for an adult to use a phone at the table if a child was present. When children inevitably violate the phone prohibition during dinner, they run the risk of fighting with their parents about these broken expectations.

There are riskier places to use a phone than the dinner table, however. Studies on texting and driving repeatedly show that texting, dialing, or using a phone for other reasons increases the risk

of accident while driving [24, 57]. Despite that, many drivers, including young drivers, engage in texting and driving [36], especially when they think the call is important [88]. Further, researchers warn that simply making texting and driving illegal is not enough to dissuade the behavior, and that additional interventions are needed to prevent drivers from using phones while driving [90].

It is unsurprising that parents often struggle to control their children's usage, given the amount of trouble that adults seem to have managing their own usage. Multiple studies examine the challenges that adults have in managing technology boundaries—e.g., checking work emails on the toilet and at the dinner table [25] or getting "lost" in email [45]. Some adults also report struggles to control the boundary between work and home, especially when required to use personal devices for work tasks [38].

Children's usage may be influenced by their parents' behaviors. Lauricella et al. [62] report that, based on examining a representative sample of over 2,300 parents of young children (ages 0-8), children's screen time is strongly associated with parents' own screen time and is highly influenced by parents' attitudes.

Furthermore, parents may be limited by their own levels of knowledge about the technologies that their children are using. Yardi and Bruckman, in a 2011 paper, interviewed 16 parents and found that parents often had or perceived themselves to have technology knowledge gaps as compared to their children, which negatively impacted parents' ability to create meaningful rules about how their children could use technology [140]. The authors suggest that parents need to understand what their children do online as a first step towards creating authoritative limits.

Time and contexts of technology use are not, of course, the only concerns of modern parents surrounding technology, and families also employ a variety of strategies to attempt to ensure online safety. However, just as inflexible context-based restrictions of phone use often fail, restricting digital behaviors may not reduce risk, and risk experience may protect children against future risk. Through a secondary analysis of Pew Research survey data, Jia et al. developed a model of teen online behavior that suggests teens who experience some risk are also likely to develop risk-coping behaviors [53]. Wisniewski et al. followed this study with a survey of 75 teens, and found that resilience helped inoculate teens against risk and addictive behavior patterns [131]. This work corroborated earlier work by Livingstone about the importance of risk-taking for teens developing their public and private identities online [69].

Certain types of risks dominated earlier studies of children's online safety. Sonia Livingstone has studied online risks to children in the European Union for over a decade. In a 2008 review of pre-existing literature, she and Leslie Haddon described a research landscape focusing on 'content' and 'contact' risks [72]. The prevalences of these categories of risks was later revisited in another survey, which highlighted pornography, sexting, bullying, and meeting online contacts as top-of-mind for children [73] Despite the common concern about these types of risks, Livingstone and Smith found that they affect less than 20% of teens, and those rates were not rising with the use of mobile technology [75]. In fact, national research suggests that child abduction by a stranger, met either online or offline, occured to about 100 children in 2011, and that number has held steady since at least the late 1990s [137]. In comparison, the same study found that over 200,000 children were reported missing in 2011 [109]. Children in the United States are not likely to be victims of "stereotypical kidnapping" by a stranger they met online.

A meta-analysis of adolescent online communication from 2010 noted the prevalence of cyber-bullying and online sexual solicitation, but continued that a number of factors influenced whether and how adolescents experienced those risks, including when the study took place [122]. In particular, earlier studies found more negative effects. This finding hints at how much internet use changed from the mid-1990s to 2010, and further change in the years since indicates that researchers must continue to re-evaluate adolescent online risks.

However, some groups of children are more susceptible to risks than others. Young people who are sexual minorities are at higher risk for suicide and have higher rates of internet use, making social media an important space for reaching and intervening with this population [110], and conversely, victimization, which can take place online, may increase a person's risk for suicidal ideation and self-harm [68].

6.1.4   Challenges of Studying Adolescent Risky Online Behavior

It is challenging to study the risks facing children and teens online. The relevancy of studies expires quickly, and studying families poses significant methodological problems; together, these have resulted in few longitudinal studies and few studies involving both parents and children, especially from the same family [72].

Many studies in this space focus only risks, and not children's experiences of harm or risk prevention efforts, which can create an exaggerated panic about those risks. Livingstone writes: "public perceptions may conclude that all children are 'at risk'... that result in anxious calls to restrict children's internet access, increase surveillance or legislate against online freedoms" [70].

Further, online risks may be and unavoidable part of the landscape of children using the internet. Livingstone and Helsper examined the tradeoffs of online risks and safety measures and found that online opportunities—learning, creativity, entertainment, etc.—were correlated with online risks. If a teen took up more online opportunities, they also experienced more risks. They did not find that internet literacy reduced risk experiences [74].

In the remainder of this chapter, we present findings from our study, which addressed many of these challenges.

6.2   Results

In this section, we describe the findings from our analyses of participants' responses to questions about internet safety risks from both interview and survey studies. The methodology used for the analyses we present in this chapter is detailed in section 4.5.2. Here, we discuss participants' perceptions of online safety risks and how those perceptions did not change despite the introduction of either the parental control software or the behavior contract. We also note two specific risks, cyberbullying and screen time, and discuss them in further detail.

Full results of the statistical models discussed below can be found in the Appendix, Tables F.1, F.2, F.3, and F.4.

6.2.1   Evaluations of Risk Attributes: Likelihood, Severity, and Confidence in Parent and Child to Prevent Risks

As discussed in section 4.5.2, we developed two statistical models of participants' perceptions of online safety risks. In the first, we examined the entire data set, but did not include interactions with study condition. In the second, we examined primarily the interactions of condition and other study variables. We present the results of both in the sections below. In total, we asked about 13 risks in the interview study and 18 risks in the survey study, for a combined total of 21 unique risks. Each risk was evaluated on four attributes: likelihood, severity, parent's ability to prevent the risk, and child's ability to prevent the risk. Figure 6.2 shows the mean likelihood and severity ratings of each of the 21 risks.
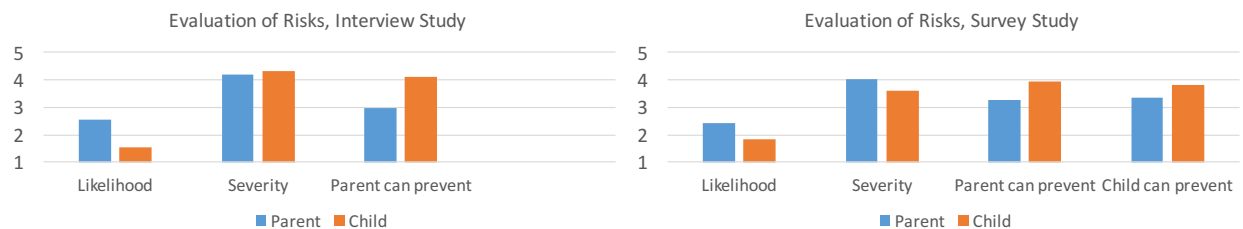
Figure 6.1: Comparisons of means for the attributes on which each risk was evaluated, across parent and child. The left panel displays these means for the interview study, and the right panel displays the same for the survey study. We can see that likelihood was rated much lower than severity by both parents and children. Parents rated their confidence in their (interviews and surveys) and their child's (surveys only) ability to prevent these risks from happening only slightly higher than they rated the likelihood of a risk happening; children thought risks were very preventable and very unlikely.

Risk Severity

In general, participants in our studies rated risks as severe, though severity was more pronounced for our interview participants than our survey participants. Overall, parents in our interview study had a much smaller difference between their ratings of likelihood and severity than did children ($p = 0.010$). In other words, children thought that the risks presented were very unlikely and highly severe, whereas parents' ratings of severity were not as extreme a jump from their estimations of risk likelihood. This was particularly true for parents' severity ratings of illegal downloads ($p = 0.008$) and viruses ($p = 0.001$), as well as the risk of worsening interpersonal relationships due to time spent online ($p = 0.003$). This was not replicated in the survey study ($p = 0.683$). As we can see in Figure 6.1, both groups of participants rated risks as more severe in the interview study as compared to the survey study.

Prevention of Risk

We found that parents in both of our studies rated their own ability to protect their children from online safety risks lower than their children did, when controlling for the ratings of likelihood of the risks. What this means is that children trusted their parents to keep them safe more than parents felt confident in their own ability to do so. This pattern was true in both the interview and survey studies, suggesting that it is a robust finding.

Parents in the interview study were more likely to rate their ability to protect their child from online risks lower than children did ($p < 0.001$). Parents were specifically less confident in their ability to protect their children from being cyberbullied than were children ($p = 0.004$). As with severity, parents were also less confident in protecting their children from illegal downloading ($p = 0.012$) and viruses ($p = 0.008$).

Survey study parents rated their ability to protect their child from any risk significantly lower than their children did ($p < 0.001$), indicating a particular gap between children's trust in parental protection and parents' confidence in providing that protection. Parents were less confident that they could protect their children from accidental exposure to adult content ($p < 0.001$) or drugs- and alcohol-related content ($p = 0.003$), viruses ($p < 0.001$), spending too much time online ($p = 0.004$), and being cyberbullied ($p < 0.001$).

Although there was not a significant difference across all risks in the survey study in how parents
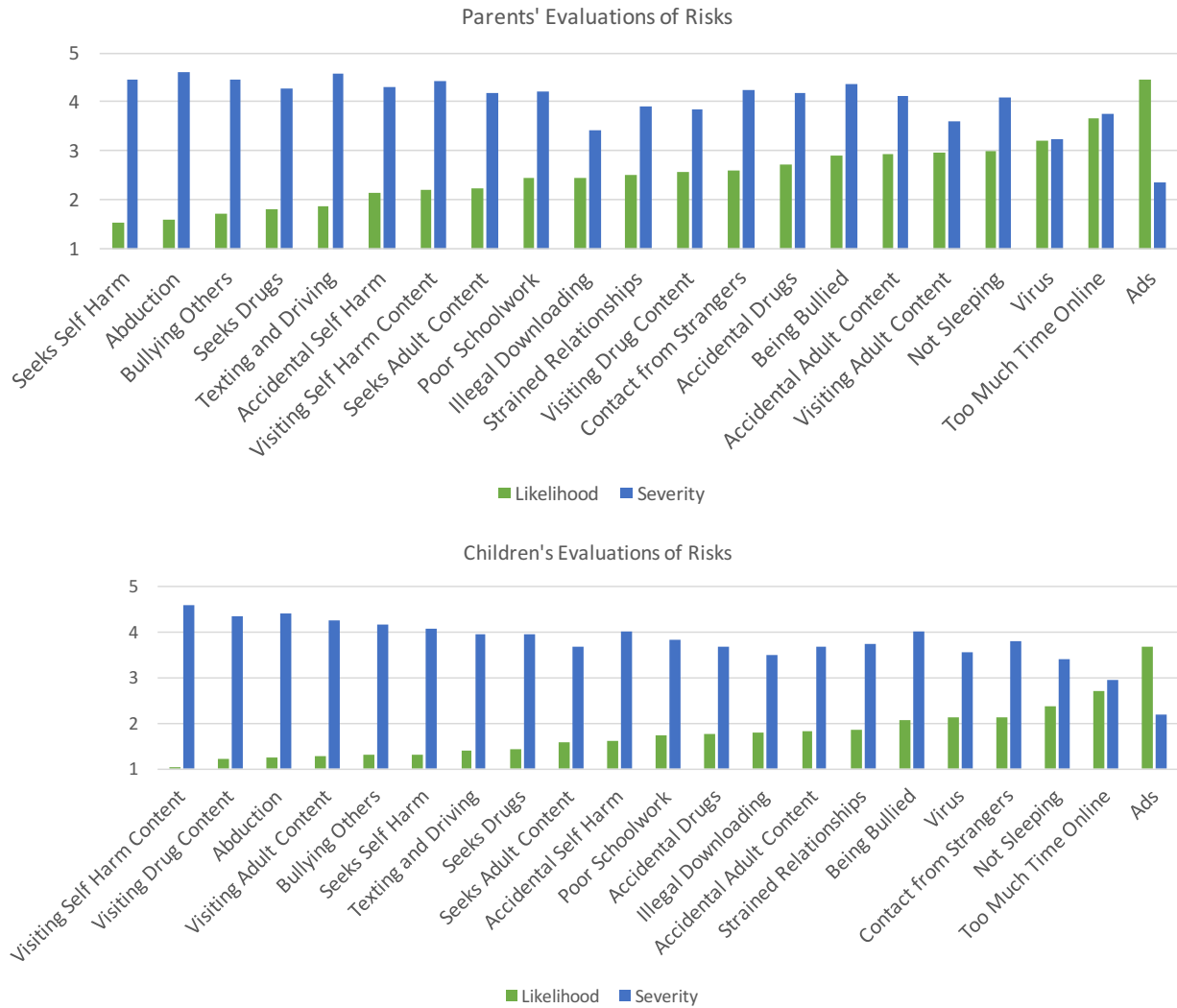
Figure 6.2: These graphs highlight parents' (top panel) and children's (bottom panel) evaluations of the severity and likelihood of risk, sorted by increasing likelihood. Parent and child data were combined across interview and survey participants due to similarity. We see that as likelihood increases, severity roughly decreases. Additionally, children's ratings of likelihood are very low for most risks.

and children rated children's ability to protect themselves from online risks ($p = 0.101$), specific risks did echo the findings about parents' ability to protect children. Parents were less confident in their child's ability to protect themselves from accidental exposure to adult content ($p < 0.001$) or drugs- and alcohol-related content ($p = 0.002$), viruses ($p < 0.001$), spending too much time online ($p < 0.001$), and being cyberbullied ($p = 0.003$). Further analysis of the final set of survey data may clarify whether parents' confidence in children is significantly lower across all risks or whether it is confined to specific risks.

Interestingly, in both cases, survey study parents and children did not significantly differ in their ratings of parents' ability to protect children ($p = 0.970$) and children's ability to protect themselves ($p = 0.436$) from bullying another child.

6.2.2 Effect of Study Condition on Risk Perception

Overall, we did not find a robust effect of study condition on participants' evaluations of risks—our experimental conditions did not seem to change how parents or children perceived risks, even though they had a new strategy to help reduce risk experiences. We expected to see that the experimental conditions had some effect on risk perceptions: Qustodio offered means to restrict children's web browsing, app usage, and screen time (detailed further in Chapter 7), and it would have made sense to see that parents or children felt differently about their ability to prevent those risks after using the tool for a month. However, our results do not paint that picture: the few significant interactions of condition, risk, and attribute or condition, participant, and attribute from the interview study are not replicated by the survey study, and most of the interactions are not significant at $\alpha = 0.05$.

This is possibly due to small sample sizes and probable inconsistent use of the tool within each family. We could not guarantee regular or consistent use of tools either within or across participating families, which is particularly notable for participants using the behavior contract. If we could guarantee this, we would not be observing a realistic use case.

The full models can be found in the Appendix, in Table F.3 and Table F.4.

6.2.3 Sexual Predators

Sexual predation and related worries about malicious strangers one might meet online were a consistent concern for our survey participants. Interview participants mentioned sexual predators during the entrance interviews, but this risk largely disappeared by the time of the exit interview discussions, replaced by concerns over screen time. However, online predators remained the most discussed risk for survey participants in both entrance and exit surveys.

Many of these participants, both parents and children, wrote simply "predators" or similar when asked about online risks that concerned them. These one-word or phrase answers do indicate that online predators may be a top-of-mind risk for families despite actual occurrences of typical "stranger danger" encounters being very low, as mentioned in section 6.1. Still, many participants did not elaborate beyond stating the concept of online predators as a risk, and so it is difficult to gauge whether this risk was just the most obvious way to answer the question or whether it was more specifically significant to these families.

6.2.4 Adult Content

Our survey study participants were similarly highly concerned about children accessing adult content online both in the entrance and exit surveys. Interview participant concern about adult content was again less prevalent in our exit interviews as participants largely opted to discuss screen time.

Some of our interview participants did share their or their child's run-ins with adult content in their weekly survey responses, despite that.

As described above, our survey participants largely opted to indicate that adult content, pornography, violence, and inappropriate language were generally concerning, but did not elaborate on these risks.

We received a handful of weekly check-in reports from out interview participants describing an encounter with adult content. In many of these, children reported coming across something accidentally and deleting the content or closing out the page without telling a parent. An 18-year-old girl explained that she didn't tell a parent about the incident because she could "handle it [her]self." In one notable incident, however, a mother of a 14-year-old boy reported that her son had tried to access pornography and been blocked by Qustodio, which then alerted her of the incident. She ended up taking away her son's phone as a punishment for his attempted actions. Here, Qustodio enabled the mother to be aware of the content her son was viewing and stop it; his actions may not have been blocked or noticed without the software in place. In this respect, Qustodio was successful at preventing what one family defined as a negative behavior.

6.2.5 Cyberbullying

As discussed in Chapter 5, cyberbullying was investigated in both the interview and survey studies. For a full analysis of perceptions of cyberbullying, please refer to that chapter. We note here that both the risk of the child being bullied and the child bullying others were rated as highly severe by both parents and children, with mean ratings above four on a five-point scale, as shown in Figure 6.2. Despite high levels of concern about bullying among our participants, neither of the tools tested sufficiently addressed the associated risks. Qustodio did not mention bullying anywhere, and The Smart Talk only touched on the topic of bullying briefly, in the form of asking the child to promise they would treat others with respect. As was detailed in Chapter 5, the sole severe risk incident during our study dealt with cyberbullying, though the family in which it occurred was assigned to the control condition. The lack of focus on cyberbullying in both tools was very different from the amount of focus given by the tools to screen time, which was an emergent concern for our participants and is discussed below.

6.2.6 Screen Time

During our interview study, we sent out weekly surveys in which parents and children were asked to give short updates about the child's use of the internet during the past week. We were surprised to find that, despite families giving a range of concerns during the initial interviews, many of the weekly reports centered on the amount of time the child spent on their phone. A mother of an 18-year-old girl complained about her daughter "using it excessively," and another mother was dismayed that that her 14-year-old daughter was "spending so much time looking at her mobile device or laptop." These incidents were often arguments between the parent and child.

Our exit interviews with participants yielded the same results. Time spent online was the most-discussed risk, along with negative social impacts from spending too much time online. Typically, a participant would express that there was an argument, or someone got upset or angry, about how much time the child spent using their phone. Screen time emerged as a daily concern for most families. As one 14-year-old girl put it, "I just kind of am always on my phone." Some families reported changing the time limits in Qustodio in response to a child's behavior, both allowing more time after some discussion and further restricting time in response to bad behavior; families assigned to use The Smart Talk more rarely reported returning to their contract, and even then
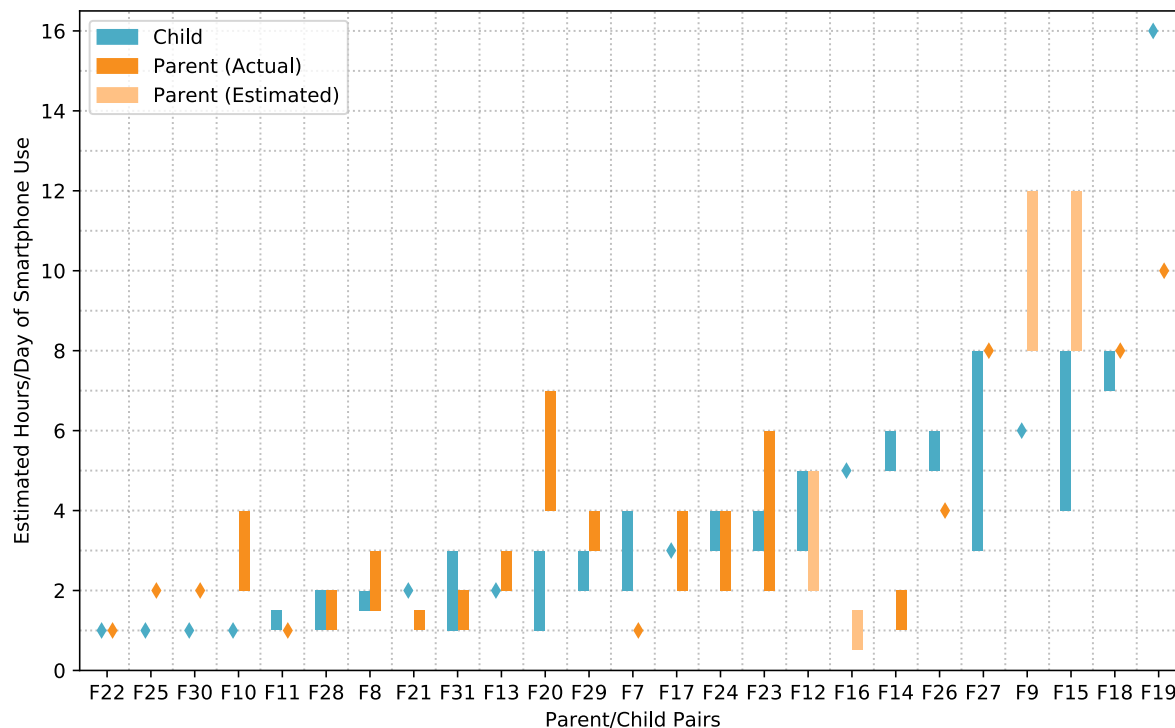
Figure 6.3: Estimated number of hours per day of smartphone use for both parents and children in the interview study. Note that six families in this study were not asked this question. Some parents responded using phrases (e.g. "all day"), rather than numerical estimates, which we translated to numerical estimates as indicated by the lighter orange bars. Parents and children provided similar estimates at the lower end of the spectrum, and those estimates diverged at the higher end.

only as a reference for the rules that had been set. Most families, when reporting incidents of screen time disagreements, cited just discussion or no tool at all as being used to resolve the disagreement.

As a result of our observations about screen time during our interview study, we added screen time as a risk, in and of itself, in the surveys given to participants in our survey study. We did so because families discussed screen time separately from associated risks, like poor academic performance due to time spent online—though spending a lot of time online might result in many other consequences for a child, families focused on the amount of time to the exclusion of these consequences.

Usage Estimates from Parents and Children

Following the identification of screen time as a distinct risk, we also began systematically asking participants in the interview study to estimate how much time the child spent using their phone every day, and continued this in the survey. We asked parents and children to make this estimation separately. We asked both parents and children to estimate the number of hours per day that the child used their phone, and many participants responded with a range. In order to analyze these ranges alongside single-number estimates, we averaged the endpoints to obtain a midpoint of the estimated range. We combine the results of the survey and interview estimates here, though a graph of just the interview participants' responses is available in Figure 6.3.

Children estimated an average of 3.9 hours per day (average minimum: 2.7 hours, average

maximum: 5.1 hours), and parents estimated an average of 4.0 hours per day (average minimum: 2.6 hours, average maximum: 5.4 hours). These estimates were not significantly different from each other ($p = 0.787$).

Though children and parents averaged similar overall estimates, within families, estimates of a child's smartphone use varied more. The average difference between a parent's midpoint estimate and a child's midpoint estimate was 1.8 hours per day. In only 15 families, about 12.2% of our sample, did the parent and the child have the same midpoint estimate of the number of hours of smartphone use per day.

6.3   Discussion

Past studies, discussed in section 6.1, have focused on the likelihood of risks and harm. Our findings contribute another perspective: how well can the family prevent the risk or harm? We found that parents in our studies consistently expressed a lower confidence in their ability to protect their children from online risks than did children, and similarly that parents expressed lower confidence in their children's ability to do the same for particular risks among survey participants than did children.

We cannot say how children thought they or their parents could prevent these risks. What we do know is that rules and values are not enough: young people are texting and driving, for example, despite knowing that it is an unsafe activity [36, 88]. Children might expect that because they know something is risky, they will avoid it when push comes to shove. Alternately, they might expect that their parents are more in-touch with the child's behavior than the parents feel that they are. Either way, children rated their confidence in they or their parents preventing online risks fairly highly: they expected that they would be shielded from most of these risks. This matched their low ratings of the likelihood of many of these risks occurring to them.

Parents gave much more moderate ratings of their confidence in themselves and their children. This indicates that parents are not assured that whatever risk interventions they are using will be successful. Notably, we did not see a robust, consistent pattern of parental confidence in risk prevention changing over time. If parents aren't sure that they can protect their children from online risks, and increased use of safety interventions isn't necessarily helping that, then research must investigate the causes of that confidence gap between parents and their children.

One reason parents might not be confident in their ability to protect children from online risks is that they aren't aware of a risk event before or while it happens. As with texting and driving, instilling an understanding of risks and harms in children is only one part of the equation. If the parent isn't included in the child's decision-making process around a given risk event, or is only included once a risk has been taken, they have limited ability to mitigate potential harm. It's important to recognize that in situations where a child has the ability to make their own choice, there's always the chance they engage in risks of which the parent may not approve.

Engagement in risky behavior is a seemingly necessary part of using the internet [74]. We recognize that different risks carry different severities. The harms of meeting a stranger from the internet are necessarily different than those of staying up late watching YouTube. We suggest that future work in this area leverages the differences in likelihood and severity of various risks to tailor safety interventions. Texting and driving carries the weight of serious harms to the teen driver and others around their vehicle, and a software intervention set by a parent that removes the child's choice to text while driving might be an appropriate option for many families. On the other hand, interventions aimed at screen time might do better to build in negotiation features for the number of hours of phone use per day, thereby cutting down on arguments between parent and child in

exchange for a potentially minimal increase in risk.

We also acknowledge that the child's age may affect how they and their parents perceive risks. Texting and driving is a prime example: families with children under 16 years old could only respond to that risk hypothetically. Age could also have impacted how parents configured the tools and the impact of the tools. In Chapters 2 and 3, we regularly heard the opinion that parenting strategies should change with the child's age and maturity levels. Our current sample size is not sufficiently large enough to identify age-related effects on risk perception, but in future analyses, we hope to explore this further.

Chapter 7

Usability of Parenting Tools

7.1 Introduction and Background

Parents employ a variety of strategies to attempt to manage their teenagers' online safety. Pew reported on a national survey of parents that found over 50% had engaged in monitoring their teens' online behavior, of whom 55% had limits in place for the amount of time or times of day that their children could use the internet [9]. Many parents are actively using strategies intended to moderate their children's digital behavior. In this chapter, we examine two parenting tools, a parental control software and a behavior contract, which are used by families in an effort to prevent the risks described in the previous two chapters.

7.1.1 Rules and Restrictions in the Home

One of the most commonly-discussed digital parenting strategies throughout our studies has been the use of rules and limitations around digital behavior. Negotiating rules with children is a parenting strategy endorsed by the American Academy of Pediatrics [94], and research has shown that families desire limits based around mutual understandings of acceptable behavior [15].

However, rule-setting is also characterized by disappointing performance in many families. Mazmanian and Lanette [84] conducted a two-year ethnographic study of nine families in which they observed that parents' restrictions on children's technology use were often bent to allow for more use. Actual parenting behaviors did not line up well to the ideal of a set amount of technology use per day, which resulted in parental feelings of guilt and shame. A survey of parent-child pairs categorized rules about children's technology use into "context constraints" (e.g., forbidding phone use at the dinner table) and "activity constraints" (e.g., forbidding use of a particular app) [51]. The authors of this study found that children were less likely to follow rules that restricted usage by *context* than to follow rules that constrained technology *activities*. Further, Blackwell et al. [15] report, from interviewing 18 parent-child pairs, that families struggle to agree on contextual rules and to achieve mutual understanding of when technology use is and is not acceptable.

The challenges faced by families in their attempts to manage technology usage are not unique to North American families and have been studied in other cultural contexts with similar results. For example, Lee et al. [63] surveyed Korean children to investigate whether internet use affected family time and communication, and to explore how parental strategies related to children's internet activities. They found that two parenting techniques—recommending useful websites and co-using—were positively correlated with the frequency with which children engaged in educational activities online. Additionally, they found that parents' time and website restrictions did not affect

children's internet usage, which is consistent with many of the findings among American families that indicate difficulty in enforcing household rules and restrictions around technology use.

7.1.2 Parenting and Time Management Software

Because research suggests that families are often unsuccessful in banning devices in specific contexts, such as mealtime, systems that integrate smartphones into mealtime may be more effective at promoting family time. Ferdous et al. [37] tested a newly-designed system called TableTalk, a communal display that encourages family interaction through sharing media with each other at mealtime. They found that the prototype promoted conversation and togetherness in all nine families studied, from various backgrounds.

Some research suggests that communities may be able to encourage reduced technology use by abstaining from technology and engaging in an alternative activity together. In a 2007 paper, Woodruff et al. studied how 20 American Orthodox Jewish families used home automation technologies to enable their observance of the Sabbath [138]. The authors found that their participants appreciated the Sabbath as a respite from technology use, and in particular, they suggested that the shared community experience of abstaining from technology may be more effective than individual or even household attempts to do the same. Though their study focused on a religious group, their design suggestions may be similarly considered for children in any community. A regular community effort to encourage children to play in a local park one day each week could be similarly effective at reducing technology use in that community. Some parent communities have begun exploring similar community initiatives, such as the Wait Until 8th, which encourages parents to delay giving children a smartphone until at least 8th grade.[1]

Parenting software provides a reliable way for parents to enforce household rules—instead of a parent giving in to an argument about screen time, the software simply shuts the child's device off. However, these tools are imperfect. Wisniewski et al. investigated mobile parental control software in a survey of Android apps, and they found a "staggering imbalance" between the large number of apps that offer restriction or monitoring features to parents and the small number of apps that promote teen self-regulation [130]. This current gap in the market suggests that parenting software developers largely do not see children as primary users of their product, even though it is installed on the child's own device.

Researchers have also tested a variety of tools to assist adults with managing their use of computers and smartphones. This research not only highlights that adults struggle to manage their usage but also provides information that may be useful for design of tools aimed at children. Hiniker et al. [50] designed an application called "MyTime" intended to assist adult users reduce smartphone use and tested it with 23 adult participants (mean age 33.5). They report that this self-monitoring tool led to decreases in the amount of time that users spent on apps that they considered poor uses of time, although the amount of time that users spent using what they considered productive apps was unchanged. Additional research would help to determine whether such self-awareness tools could also benefit teenagers in decreasing non-productive smartphone usage.

Rooksby et al. tested an application called ScreenLife that allowed users to monitor their own screen time [106]. The authors deployed this application to 21 users for one month. They reported that screen time tracking might be used for varied purposes, including decreasing usage or increasing productivity. They highlighted the concern that their design decisions may have influenced users' concepts of screen time; in one case, the researchers' choice to depict time as hourly blocks, and

---

[1]https://www.waituntil8th.org/

change the color of those blocks if the phone was accessed at all during that hour, shaped users' understanding of how much and how frequently they used their phone. A different presentation that focused on minutes per day of phone use may have produced different reactions from participants. This suggests that entities developing parental control software or software to assist teenagers with managing their device usage should also consider how usage data is parsed and presented.

7.1.3 Content Filtering

Filtering or blocking websites based on their content has been an ongoing challenge since the early days of the internet. In 1995, the World Wide Wed Consortium published a specification entitled "Platform for Internet Content Selection" (PICS), which was designed explicitly to help adults control what content children saw on the internet.[2] PICS was described as "value neutral" because its framework for labeling web content could be used to achieve any goals, and was envisioned to be adaptable to different families and contexts [102]. Further, this platform was promoted at the time as a solution that "enables users to control what they receive" on the internet, rather than using legislation to censor what content is allowed to exist online [101]. Around the same time as PICS was being developed, many other content filtering solutions were on the market. This was a key component of the *ACLU v. Reno* case, which successfully overturned a U.S. legislative effort called the Communications Decency Act by arguing that regulating the internet violated free speech, especially when technological solutions for protecting kids and preserving speech existed [127].

However, the United States had many other legislative efforts around the turn of the millennium aimed at minimizing children's exposure to adult internet content [1, 2, 3]. Legislators and legal professionals wanted technological solutions to prevent minors from being exposed to pornography online [143], but contemporaneous studies of filtering and blocking software showed that these tools often did not block many websites with pornographic content [52], but did block some types of appropriate content a child might need for homework assignments [86] and health information [103]. Beyond false positives, it is worth noting that the types of content filtered by programs are the product of value judgments, from ratings of the severity of the content to decisions about what types of content should even be blocked.

7.1.4 Software Usability, Beyond Parenting

Additionally, general usability research has contributed lessons important to the design of any software, especially those with high-level permissions that significantly alter the function of the device such as parental control software.

Parenting tools may have to convey important information to users when those users are configuring settings. Research on security warnings has shown that users often do not fully read information presented to them, even when it is important, and that warnings and notices often include unnecessary information alongside the key ideas [19]. However, user attention to security warnings can be improved through interface improvements [18, 20, 34].

In the remainder of this chapter, we explore the usability of two parenting tools: a parental control software, Qustodio, and a behavior contract, The Smart Talk. Both provided a high degree of configurability to families in order to reflect the varied rules and limits parents and children might need. Both structure the process in order to provide more direction than a normal conversation. And, as we will see, both were substantially affected by usability issues.

---

[2]https://www.w3.org/PICS/

7.2 Results

As described in section 4.3.1 above, we observed 10 families set up the Qustodio parenting software and an additional 10 families set up The Smart Talk contract in the lab. We explored the usability of the different features offered by each tool and the challenges that they may pose to families. Below, we discuss issues with the user interfaces, the capabilities of each tool, and the negative experiences of participants.

7.2.1 User Interface Issues: Ambiguous or Subpar Instructions

Qustodio and The Smart Talk both relied on users dedicating a focused block of time to setting up the tool. They asked for a lot of buy-in from users: Qustodio had seven pages of settings and The Smart Talk offered 41 prompts. However, both at turns understated and under-explained the settings and prompts shown to users or under-valued the participation of either parent or child, which caused confusion or frustration as our participants grappled with how to progress through the configuration process.

Qustodio

Beginning the Installation   Qustodio began its installation process in a way that clearly underscored the central role of the parent and de-emphasized the child's agency. The site instructed users to "grab your child's device" in order to install the monitoring app, which one mother of a 15-year-old boy explicitly noted was aggressive language. Qustodio thus frames itself as software for primarily the parent's benefit from the very start.

Qustodio would not function properly if installed on a device with another parental control software already active. One mother had to disable her pre-existing installation of OurPact on her 13-year-old son's phone in order to complete the Qustodio installation. Despite this incompatibility, Qustodio did not warn users in advance that they should disable other similar software.

Some participants were disoriented when prompted to log in to the parent's Qustodio account on the child's device in order to complete the installation. The Qustodio app on the child's device asks whether the user has an account or would like to create a new account; the app does not specify that this question is directed to the parent. One mother looked to her 15-year-old son for clarification, realizing, "Oh it has to be mine, does it?" Qustodio likely assumed that the parent would grab their child's device as instructed, but did not account for the child being present with the parent or wanting to maintain control of their own device.

Qustodio also had a known incompatibility with certain types of WiFi connections when installed on Apple iPhones. In our first interview with a family instructed to install the software, this bug so totally derailed the experience of the mother and her 13-year-old son that they were forced to complete the settings pages without a working installation on the son's phone. Out of necessity, we included study instructions to avoid encountering the bug for all future software participants. Qustodio documented this issue on a help page[3] but did not include any such instructions as part of the installation process.

Indirectness   Many essential pieces of information in the Qustodio control panel were not clearly and centrally located. This was consistent across multiple pages. For example, in Figure 7.1, we see the call and SMS monitoring tab as set up by one of our participant families. The child in this family used an iPhone, however, her mother had turned on the two features shown despite those

---

[3]https://www.qustodio.com/en/help/article/2065678/
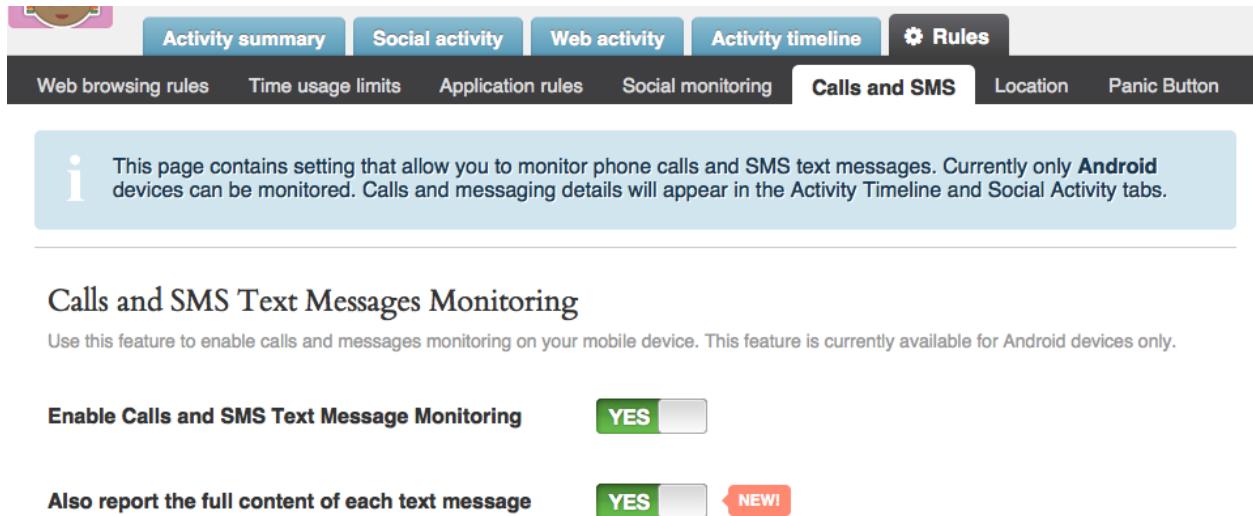
Figure 7.1: Participants often did not understand that a feature only worked on Android phones, sometimes debating whether to use the feature for minutes before realizing, or not realizing at all. This family set up Call and SMS monitoring, despite the daughter owning an iPhone. Note that the Android-only warnings are buried among text with other content.

features only working for Android phones. Qustodio mentions that these features are for Androids twice on the page: once, in the blue panel just under the tabs; and once, just underneath the text heading, in light gray text. Both of these mentions are bundled with unrelated, and repetitive, information which the parent often decided to skip reading. The panic button page was another such example, as seen in Figure 7.2. This page clarifies that the feature is Android-only in only the same two locations, but does not bold Android in the first mention. A comparatively attention-grabbing notice is devoted to the legal disclaimer that Qustodio's panic button does not replace contacting emergency services, however.

Inconsistency   In another case, an icon was inconsistently used across settings pages, which caused similar confusion to the indirect language discussed above. Figure 7.3 shows the interface parents could use to set per-day time limits for their child's device. One mother of a 13-year-old girl repeatedly attempted to click the clock icon to set a time allowance. Her daughter had to remind her where to click: "Mom, icon." The clock icon shown here is a static image, however, and the light gray text next to it is the clickable object. The settings page following the time limits page was one used to restrict specific applications, which is excerpted in Figure 7.4. Notably, a user does click the image of the clock on this page in order to set a time allowance for a specific application. Qustodio should instead consistently treat elements as interactive or static, regardless of on which page they are used.

Content Filtering   The first settings page that families would see was the web-blocking page, which is excerpted in Figure 7.5. These categories of websites were configurable by parents to be allowed, completely blocked, or accessible but the parent would receive an email when something in that category was accessed.

The categories used in the website blocking menu were not sufficiently explained. Nobody in the study could understand what was meant by "loopholes." Qustodio does not define these

Figure 7.2: This page allows parents to activate the panic button feature. Note that only italicized light gray text indicates this is an Android-only feature. Also note that the page focuses on teaching the child how to activate the panic button, but does not educate the parent on where to look for panic alerts or find the child's location.

Time allowance

Use the controls below to set a daily time allowance for your child's devices. Once your child reaches their daily quota, access will be restricted as specified in "Device lock type" until the next day. To fully restrict access for one day set the time allowance to zero.

Monday   Click to set a time allowance

Tuesday   Click to set a time allowance

Wednesday   Click to set a time allowance

Thursday   Click to set a time allowance

Friday   Click to set a time allowance

Saturday   Click to set a time allowance

Sunday   Click to set a time allowance

(*) Note: Time allowance for iOS is currently in Beta. **Read more.**

Figure 7.3: This menu allows parents to set device time limits on a per-day basis. Parents often clicked the clock icon, which is a static page element. The italicized light gray text next to the clock is clickable, and activates the time settings.

Figure 7.4: This menu allows parents to block or allow individual apps. The list of apps is populated based on the child's phone activity, and may take some time to begin appearing. Parents were confused by this menu when apps did not immediately appear, and often ignored these settings as a result. Also note the clickable clock icon, which allows parents to set individual time limits for apps.

Website categories

Use this setting to allow or restrict your child's access to specific website categories, or to receive alerts when your child accessed a site in a specific category.

Enable website category restrictions [YES]

- Educational
- Government
- Entertainment
- Search Portal
- News
- Sports
- Business
- Health

- Technology
- Games
- Travel
- Religion
- Shopping
- Employment
- Webmail
- Forums

- Social Network
- Chat
- File Sharing
- Gambling
- Loopholes
- Violence
- Weapons
- Profanity

- Mature Content
- Pornography
- Alcohol
- Drugs
- Tobacco

set all as: **Allow Alert Block**
Restore default values

Figure 7.5: This menu allows parents to block certain categories of websites from being accessed by their child's device, and the above is the default configuration. Qustodio did not provide any definitions of these terms or explanations of how offending content was blocked. Additionally, some parents were confused about the meaning of the red bars because no legend was provided.

categories—a user cannot hover over them to see the meaning or click some part of the interface to bring up a definition. There was also seeming overlap between some of the categories. What would it mean to keep "mature content" blocked but allow "pornography?" Participants were also confused about how these category restrictions functioned, including whether they would censor profanity on a page, block inappropriate videos, or similar content-based filtering—and as discussed above in section 7.1, the effectiveness of blocking software is, at best, imperfect.

The Smart Talk

Beginning and Ending the Contract Families were often confused about how to begin and end the contract creation process. The Smart Talk's homepage, partially shown in Figure 7.6, contained a button to "Get Me Started." Clicking this began the contract process. However, five brightly colored circles above that button often drew participants' eye. In two mother-daughter pairs, one of the participants asked the other which topics they should select and attempted to click those colored circles.

The end process was similarly confusing. Participants had to click a button labeled "Make it Official" to complete the contract, but the mother of one 15-year-old child stared at the button and stated, "I don't know what that means." Additionally, the completed contract suggested that parents and children sign their names, but to do so required families to print the contract on paper. No e-signing functionality existed, though the mother of a 13-year-old boy spent a few minutes trying to find it. Aside from printing, there was no other way to save the contract: no option to email it to oneself, no link to access the contract again, nor any other options but printing.
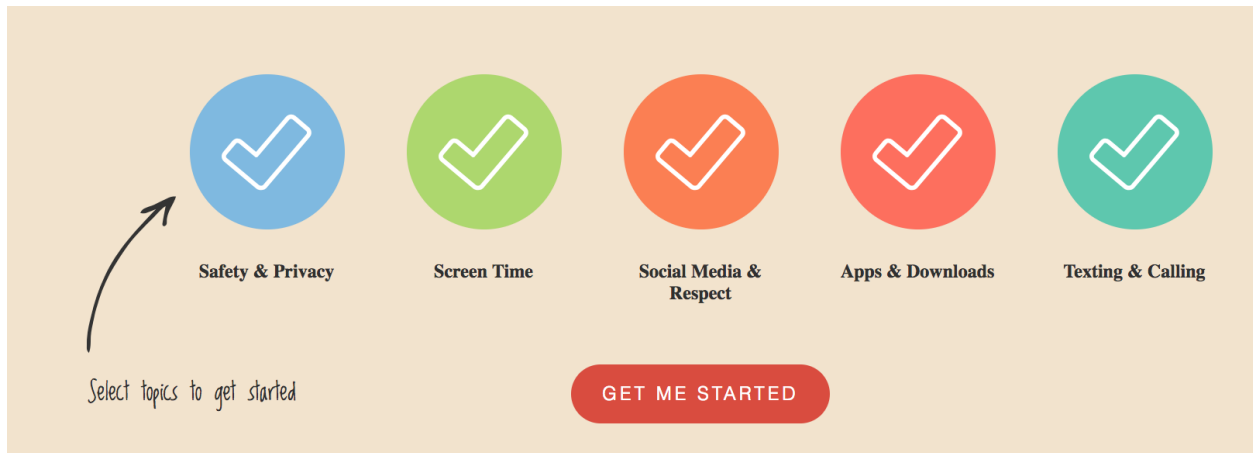
Figure 7.6: This is shown on the home page for The Smart Talk, and users select "Get Me Started" to continue. However, some participants tried to click the colorful circles above the button because of the italicized text suggesting they needed to "select topics." These icons are static page elements.
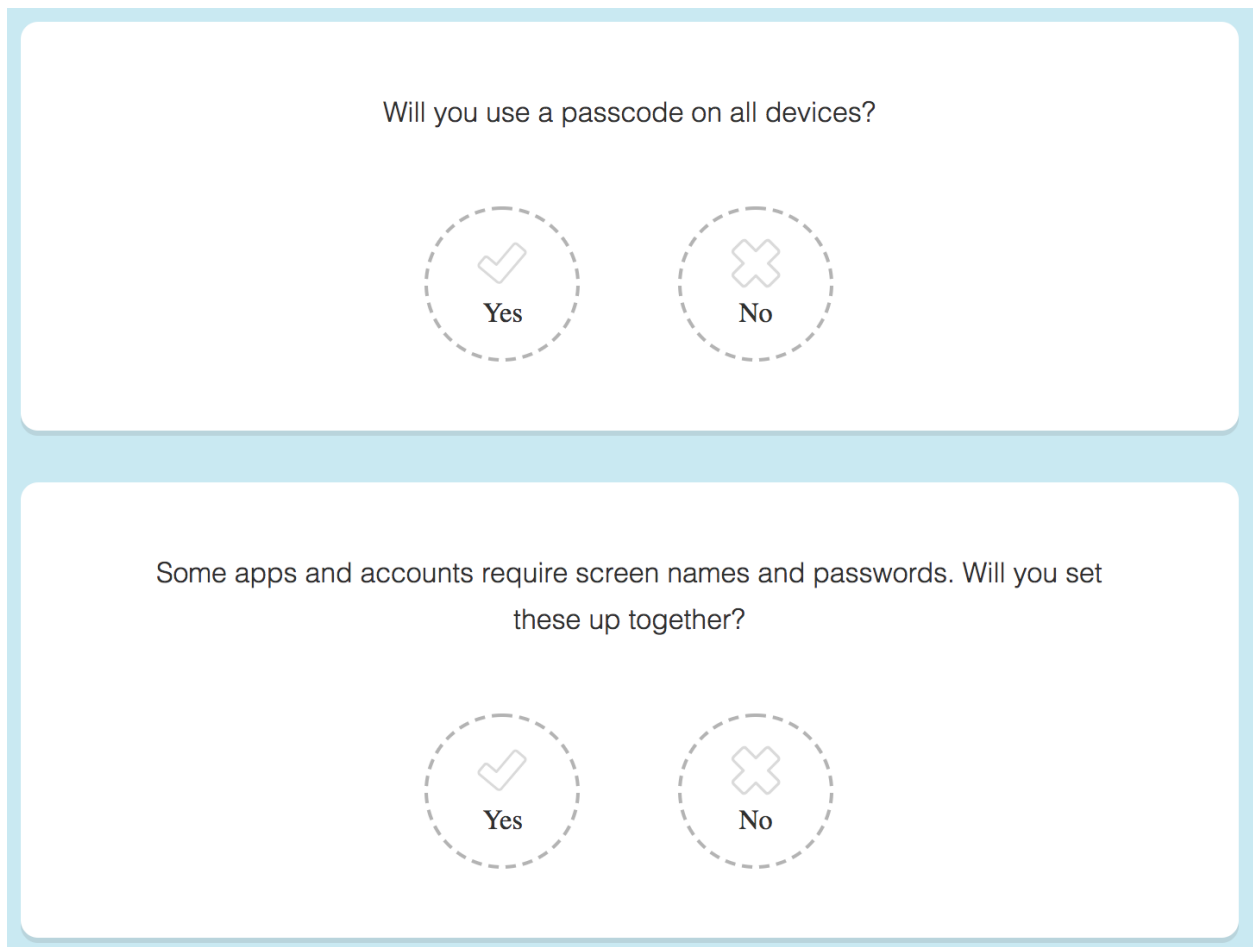
Figure 7.7: Participants were often confused about whether the parent or the child should fill out the contract questions. The ambiguous use of "you" was a particular culprit, especially when it sometimes referred to the child (top) and other times referred to both the child and the parent (bottom) in the span of two questions.

Ambiguous Terms   Families were often confused about who was supposed to answer a question in the contract. Some questions used direct language to clearly specify the subject, e.g. "[Parent], will you... ?" However, others relied only on an ambiguous "you," as shown in Figure 7.7. For example, one mother of a 13-year-old boy wondered aloud at a question about passcode use: "Will you use a passcode on all devices? Who is going to use it? Who is going to use the passcode?" Another mother of a 14-year-old boy was thrown when the subject switched between two questions. She waffled on a few interpretations before turning to the interviewer for help, saying, "No, wait a minute. I don't understand this question." The Smart Talk could have explained who was expected to be the primary respondent at the beginning of the process or used names in each question to avoid inconsistent pronoun use.

The contract makes reference to "all devices" being governed by the negotiated rules, but does not define what this phrase means nor allow the parent and child to define its meaning. One mother of a 15-year-old girl speculated, "that means house phone [and] computer, I guess?" As above, The Smart Talk could have addressed its assumptions about devices at the start of the contract, or even offered families a question in which they could choose to which devices the contract applied.

The Smart Talk used a handful of shorthand terms and colloquialisms in their contract, and though most families were not bothered by this, some were confused. In one example, the contract prompts the child to name their "#1 bestie," a term that prompted a 15-year-old girl to clarify, "like, my best friend?" An 18-year-old girl was confused when reading aloud a question that included the abbreviation IM, and she stumbled, "Uh, whatever that means."

7.2.2   Tool Capability Issues: Poorly Executed Features

Though the issues described above confused participants because features were poorly explained by the user interface, the features largely functioned as expected once one figured out the intended function. The features described in this section, however, were impacted by poor overall function.

Qustodio

Qustodio, as a software that functioned across multiple devices, contained a number of features that missed their mark. Some, such as Facebook monitoring and interstitial advertising, provided functionality that users just did not want. Others, such as the application controls and panic button, were desired features that needed additional functionality to be truly useful.

Outdated Social Media Monitoring   Qustodio did not offer parents a way to monitor any of the primary social media platforms currently used by a majority of American teens (see [10]). The software does have the ability to monitor a person's Facebook account, which can be set up on a page labeled "Social Monitoring," seen in Figure 7.8. Parents often expected this page to allow monitoring of multiple social media accounts, including the more widely-used Instagram and Snapchat. When only Facebook was possible, families complained that their child didn't use their Facebook account for much or didn't even have one. One mother of a 13-year-old boy, when faced with the Facebook monitoring feature, exclaimed: "but you don't have a Facebook account!" Others called Qustodio out-of-date. The mother of a 13-year-old girl posited, "I think this generation is more on Instagram and Snapchat. They [Qustodio] maybe haven't caught up on that yet." Another mother of a 13-year-old boy put it more bluntly: "Kids don't really use Facebook anyway. Qustodio better get with the times, man."
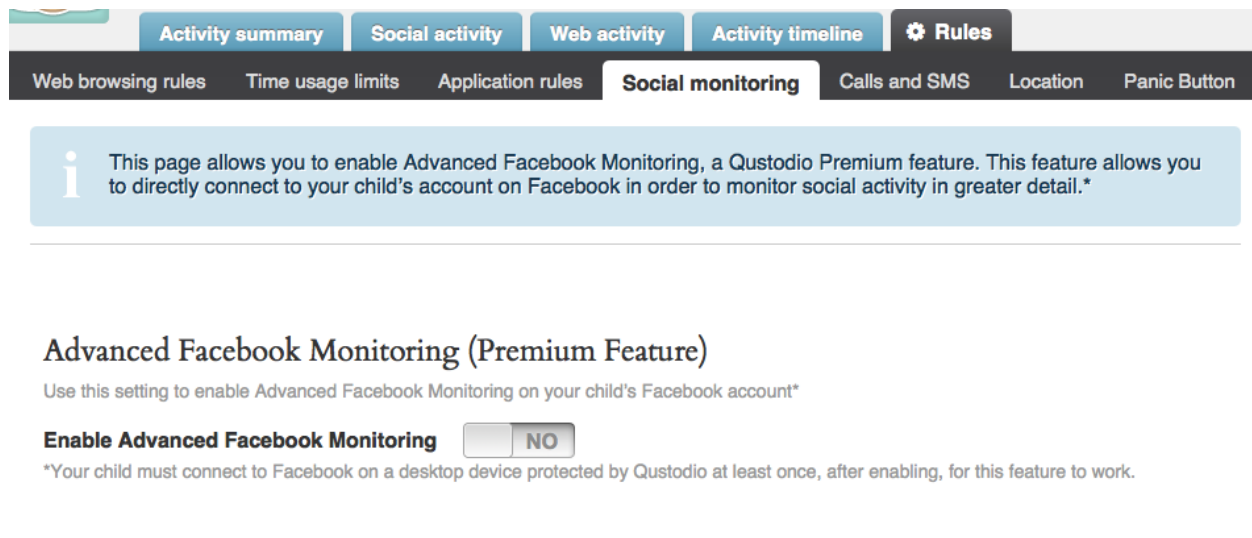
Figure 7.8: This page is used to enable Facebook account monitoring for the child. Qustodio calls this "Social Monitoring," but many parents were disappointed to see that it only applied to Facebook and not social apps like Instagram and Snapchat.

Delayed Application-Specific Features After Installation   The application controls in Qustodio require a delay before setup, and Qustodio does not sufficiently design for this configuration hurdle. The applications, which appeared in a list as shown in Figure 7.4, were identified from the child's phone activity. As such, they only started appearing as the child used the phone with Qustodio installed. This sometimes took up to an hour after the initial installation. Participants in the lab often did not have a chance to see the applications appear before the end of our interview time, and as a result, often ignored this setting altogether. The father of a 15-year-old boy remarked, upon refreshing the page, "nothing's popping up," before eventually moving on to other features. Qustodio could have drawn these users back to this page with a reminder email in a day or a week, or whenever new-to-Qustodio apps were detected on the child's device.

Interstitial Advertising   Despite our participants having Qustodio premium accounts, they were shown ads for upgrading to premium accounts, sometimes numerous times, when loading the site. This interstitial ad can be seen in Figure 7.9. In one memorable example, a mother and son, age 15, decided to test the functionality of the panic button during the interview. Upon loading the page with a live map displaying her son's location, the mother was again shown an ad for Qustodio premium, blocking her view of the page beneath. The mother mockingly exclaimed, "Stop advertising to me, my son is in danger!"

Difficulty Accessing Panic Features   The ad was the last in a long line of complications during the panic button process. When the son had first hit the panic button at the beginning of their test, Qustodio notified him that they were sending an email alert to his mother. She wondered, "why can't it just message me on my phone?" SMS messaging was an option for the panic button functionality, but by default it only sends an email alert to the email associated with the Qustodio account, and activating the panic button option did not clearly and directly prompt the parent to enter a phone number for contact. Accessing the son's location required the mother to click a link in that email and log into her Qustodio account, which she found absurd, and she complained, "I'm

94
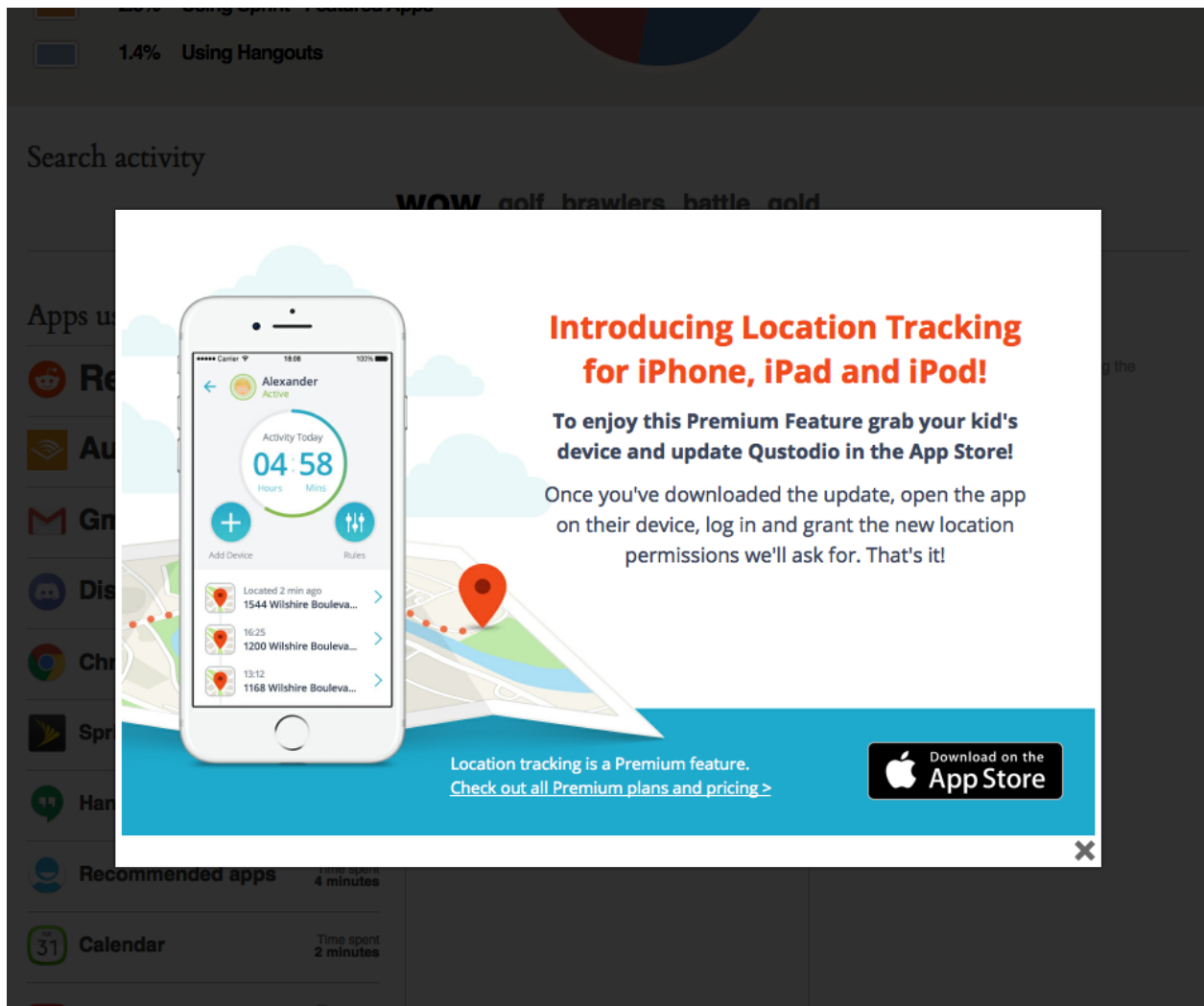
Figure 7.9: This interstitial ad was shown to users in our study, despite these users having paid Qustodio accounts. Note the content behind the ad is heavily obscured.

Smartphones and most apps come with privacy settings to protect personal info. Select who will choose privacy settings for ChildName's devices.

🔒 ChildName   ParentName

Figure 7.10: The Smart Talk included questions that required users to select either the parent or a child to be responsible for something. Families sometimes wanted to select both the parent and the child, but the interface prevented that. Some participants were also confused by the choice of a lock icon to represent the selected name.

going to spend five minutes remembering my password so I can save you."

The Smart Talk

The Smart Talk, as a text-only contract intended to prompt discussion between parent and child, did not have as many poorly-designed features as Qustodio. Nonetheless, the contract restricted some answer choices so that families could not accurately represent their desired rules, and framed a key feature, the bonus talks, in a way that led some children to not seriously engage.

Assigning Responsibilities to Both Parent and Child   The Smart Talk did not allow for selection of multiple names in questions where parent and child were asked who would be responsible for a given action. This type of question can be seen in Figure 7.10. The mother of a 15-year-old child decided she would just pretend like both names were selected, and a 12-year-old girl disclaimed, "Ugh, that's sad" when she could not select both names. Parents and children wanted to share a responsibility but could not do so given the interface.

"Bonus" Talks   One type of prompt shown to participants was the "Bonus Talk," an example of which can be seen in Figure 7.11. These prompted families to discuss a topic in more depth after setting a rule. They sometimes provided useful information, such as how to create a strong password. However, labeling them as "bonus" resulted in some children trying to skip them. One 13-year-old boy whined to his mother, "Do we have to do it?" Some children will likely want to minimize the amount of time they spend discussing online behavior with their parents, and re-labeling these helpful discussion prompts might reduce their grumbling and avoidance.

7.2.3   Parent-Child Experience: Disagreements Over Screen Time

Families in our study were consistently concerned about the amount of time that children spent using their digital devices. Both the software and contract offered tools that promised to help families manage screen time, though both were saddled with issues. Qustodio's screen time features worked: the phone went off when a parent set it to go off. However, the controls were not very adaptable and children protested this rigidity. The Smart Talk offered negotiable screen time boundaries, but these negotiations often devolved into bickering and left parents with no new tools for enforcing the agreed-upon boundaries.

Figure 7.11: A few of these bonus talks were included in the contract. Because they were called "bonuses," children sometimes argued to ignore or skip them.

Qustodio

The parental control software offered reliable enforcement of screen time limits, and most parents utilized that feature. Children had a hard time accepting those limits when the parents were configuring them, and often voiced their discomfort with their lack of control. Software-enforced time restrictions removed the child's ability to easily justify their use of a smartphone above and beyond normal limits, as the phone would be automatically disabled when the limit was reached. Parents who might want to extend their child's screen time for the day would have to access the software control panel to make changes, which was fairly uncommon for most of our participants.

In Qustodio, users are able to limit the amount of time that a device can be used in two primary ways: (1) the user can set a weekly schedule and enable or disable device use for each hour of the day individually, which allows, for example, a parent to set a device to turn off at 9:00pm during the weekdays and 10:00pm on the weekends; (2) the user can set a limit on the number of hours per day that a device can be used, again for each day of the week separately, so that a child might be enabled to use their device for two hours on weekdays and three hours on weekends. Both of these settings can be independently enabled or disabled by the user, so that use of a device might be moderated by one type of limit but not the other, both limits, or neither. We provided Qustodio for ten of our participant pairs during the period of study, and seven pairs enabled at least one of the available time restrictions. Qustodio also allowed families to time-restrict specific apps as part of the "Application Rules" page, though none of the families in our study chose to do so. As discussed above, the application settings had interface issues that may have prevented families from configuring these rules.

Five pairs of participants left the weekly schedule disabled throughout the study, four enabled it when configuring the software in the lab and left it enabled throughout the study, and one pair initially enabled the schedule, disabled it, and re-enabled it during the period of study. Participants made an average of less than one (0.7) change to the weekly schedule, and we recorded a maximum of four changes to the schedule.

For the second type of limit, five of our ten software condition participant pairs enabled a limit on the number of hours per day that the child could use their smartphone. Another four did not enable this limit during the period of study, and one pair initially left this setting disabled but enabled the hours per day limit before the end of the first week. Participants made an average of 4.2 changes to their hours per day settings with a median of zero changes (min: 0, max: 23). Parents gave their children an average of 3.2 hours of smartphone use per weekday (min: 1, max: 10)[4] and an average of 4.4 hours per weekend day (min: 2, max: 8).

Most parents were excited to see time limit settings when configuring their accounts. The mother of a 15-year-old boy exclaimed, "I could turn off your phone so you could sleep! [You could] eat dinner with me sometimes!"

Our child participants, however, were not as excited. Some children expressed their raw fear and disbelief as emotional pleas to their parents: "Nooo!," screamed a 13-year-old girl. Participants quickly turned to bargaining. Parents, such as the mother of a 12-year-old boy, would offer something they thought reasonable: "How about we start with two hours?" No matter the offer, though, their child would try to negotiate. One girl, age 14, argued that she could only stream women's soccer matches through a special app on her phone, and so her mother's proposed 90 minutes per weekday were not enough for even one game. Her mother countered: "When school starts, will you be watching soccer games during the week?"

Even once parents had set time limits for the child, questions remained about how Qustodio counted activity against the total time allowance. The mother of the same 13-year-old girl who screamed "Nooo!" when the time allowance was being configured later wondered, "If she looks at what time it is now is that considered to be usage? Like she clicks on the Home button to look at the time?" In our own testing, we found that Qustodio seemed to count time in one-minute increments on an Android phone—though this behavior may differ by platform according to Qustodio's help page.[5]

The Smart Talk

We anticipated that parents and children who set up a behavior contract might have calmer discussions about screen time than those who set up a parenting software, given the contract explicitly frames its prompts as a negotiation between both the parent and the child. Unsurprisingly, families were still reluctant to compromise. Further, the contract's prompts for specific time limits frustrated parents, who had no clear answer for how to enforce the restrictions they had created.

Families in the behavior contract condition were asked to set rules about their child's screen time as part of the process of creating the contract. The contract asked them to pick both a maximum number of hours per day that the child could use their phone and to set a morning and bedtime schedule for weekdays and weekends, as shown in Figure 7.12. In this condition, parents allowed an average of 2.95 hours of screen time per day (min: 1, max: 7). During weekdays, children were allowed to start using their phones between 5:45 am and 7:15 am, and children were to stop using their phones between 8:00 pm and 10:30 pm. During weekends, those times shifted slightly later, as expected: morning start times ranged from 6:30 am to 9:00 am, and evening end times ranged between 9:00 pm and midnight.

Picking a time in the morning when the child could begin to use their smartphone was particularly challenging for our participants because most wanted the morning time to reflect when the child wakes up, which was an especially moving target during the summer, when we conducted these interviews. One mother noted that her son, age 13, wakes up at variable hours, and another mother

---

[4]One parent increased the hours/day limit from 3 to 10 on one day of the week in advance of summer travel.
[5]https://www.qustodio.com/en/help/article/2778761/
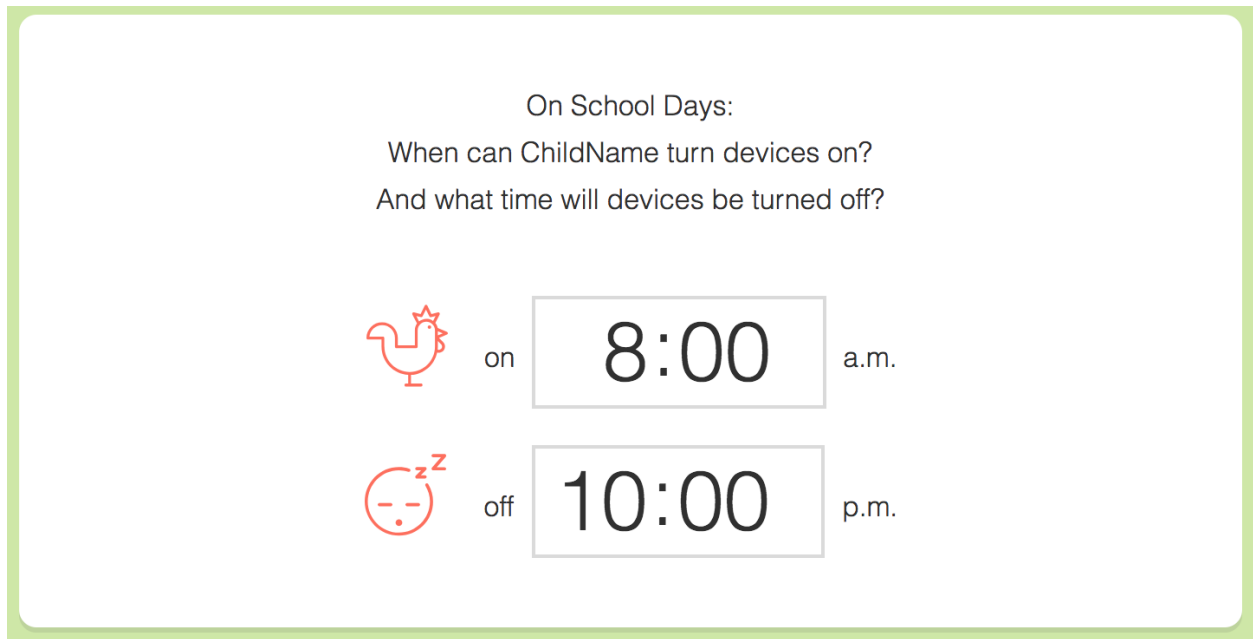
Figure 7.12: This menu prompted families to set a daily start and end time for the child's device use. Note that the question asks only about when a device can be turned on and off for the day, but the icons (rooster, sleeping face) and time indicators (a.m., p.m.) imply that families should select when the child wakes up and when they go to bed.

solved this dilemma by picking a reasonably accurate time and telling her 14-year-old daughter, "It's really when you wake up." A 10-year-old girl, was anxious about her mother selecting a later time for weekend mornings than weekday mornings, and her mother jabbed, "When are you ever up at 7:00 on the weekends?" Nevertheless, the daughter received her wish and weekend morning phone use was still allowed starting at 7:00 am.

Resistance to compromise was common among our participant pairs. One mother remarked to her 12-year-old daughter, "You want to go up, and I want to go down," as they reached a stalemate about the number of hours she could use her phone each day. Another mother of a 14-year-old girl never settled her qualms about the agreed 10:00 pm weekday bedtime, and left the interview session still questioning whether she should make it earlier. Some children resisted compromise even though the suggested rules wouldn't affect them: a boy aged 13 was an early sleeper but wanted a later bedtime on principle, and a 15-year-old girl disliked a rule banning phone use during religious services because her family did not attend any regular service.

Compounding these conflicts about the terms of the contract was some parents' distrust that their children would respect any agreement. One mother figured if her daughter was responsible for tracking her own phone use, the girl would lie that she had been on the phone only "five minutes" whenever asked. Another mother shared this exchange with her 18-year-old daughter about monitoring hours of phone use:

Mother: "How are you going to do that?"
Daughter: "I'm going to do that."
Mother: "That's not what I asked!"

Even this adult daughter, who would be heading to her first year of college in the coming fall semester, was not trusted to keep accurate track of how much time she had spent on her phone.

However, some parents were more willing to trust their child, in part due to the difficulty of keeping track of the child's screen time. One mother said she would trust her daughter, age 10, "even more" if the daughter's time limits were in a contract, and another mother only committed to having a "conversation" with her daughter, age 12, if their contract was broken. A third mother bluntly addressed the screen time agreement with her 14-year-old son: "I'm not tracking your time. You have got to be responsible for it." Regardless of whether the parent or the child was ultimately responsible for tracking the child's phone time, participants who set up a behavior contract struggled to think of a realistic way to enforce the time limits they had negotiated.

7.2.4 Responses from Survey Study

Participants in our survey study were asked to describe their experiences setting up the software or contract, though as researchers were not present to observe the process, these experiences were not captured in as much detail as those in the interview study, described above. However, we note below the main themes of our survey participants' responses.

Survey participants largely reported liking both the contract and the software, and shared positive, approving reviews of the tools. Many participants particularly described the software as easy to configure and "user friendly," and the contract as a good opportunity to have discussions with their children. Compared to the interview participants, the survey participants reported more positive feelings towards both tools.

Despite the positive feedback and less detailed reporting, we did see negative evaluations of both Qustodio and The Smart Talk in some survey responses. In particular, Qustodio was the subject of many complaints about the overwhelming setup process and confusing, unhelpful explanations; these complaints mirrored those discussed above. Participants who set up the contract noted difficulty negotiating some rules, including screen time, allowed apps, and social media usage. A mother of a 12-year-old boy called the negotiation a "very emotional process." One father of a 13-year-old boy expressed an additional concern with The Smart Talk, which expanded on the user interface issues described above: he felt that the language in the contract could be patronizing towards the child.

Overall, survey participants' positive reactions to the tools were surprising, given our observations during the interviews, and their negative reactions to the tools hewed closely to those observed during the interviews. We anticipate that survey participants' experiences with the tools were somewhat flattened compared to interview participants' experiences because many of our findings, described in this section, were based on our observations of participant behavior during the in-lab setup process rather than on self-reflection from the participants.

7.3 Discussion

The goal of studying Qustodio and The Smart Talk was to understand what their use, as examples of parental control software and online behavior contracts, could tell us about using those types of tools in general. In this section, we discuss the need for usability testing of all tools and the implications from our study for both of the categories of tools studied.

7.3.1 Importance of Usability Testing

Both the Qustodio and The Smart Talk interfaces would benefit from usability testing, which has been a widely-documented practice for software and web-based interfaces since at least the 1990s [30, 33, 41, 92, 108, 139], including specific guidelines for usability testing with children [21,

44]. The Smart Talk suffers from phrasing irregularities and unclear or frustrating functionality, and Qustodio shares the same weaknesses with the addition of installation difficulties and legibility issues. Many of these problems would be caught with usability tests of even a few users, as our own findings are based on usability tests with 10 user pairs.

7.3.2 Implications for Parental Control Software

As mentioned in Chapter 4, we chose to study Qustodio because it had capabilities typical of all leading parental control software. As a result, we can extrapolate from the issues faced by our participants to identify problems likely found in software of this type.

User Interactions

Participants in our study were installing Qustodio under ideal conditions: they were in a lab without distractions and were being paid to complete installation. We also instructed our participants to carefully read every settings page. Even then, families struggled to install the software and to understand the software settings. In real life, families will be completing this process with distractions. They may divide their configuration process into multiple periods, they may have a reluctant child, or some other complication might arise that prevents them from fully reading and processing the software settings.

Parental control software should design for this reality, and consider features that help parents navigate setup and maintenance. Qustodio and peer products send regular email reports of the child's activity to parents; email updates could also include reminders to change default settings or to look at pages that might have changed since the parent last accessed them.

Capabilities

Some features offered by Qustodio and its peers address commonly-expressed parenting needs—the ability to block certain types of online content, for example, or to monitor a child's communication and social activity. However, these features are often imperfect. For example, a parent who wants content blocked on their child's device likely wants all content of that type blocked, regardless of on which app it's accessed. Qustodio, like most parental controls, blocks content in standard web browsers only using web domains.[6] If a child was texted an inappropriate picture, or saw something on a social media app, the parental controls would have no way of filtering it. Likewise, parents who want to monitor their children's social media activity likely want to monitor all social media, not just Facebook. Some companies have released parental control software that tries to address these needs,[7,8] but this capability is not widespread. For the most part, parents do not have the choice to monitor or limit their children's online activity in the way that they want.

Rule Enforcement

Qustodio's settings were strictly enforced once set, which made the software difficult to adapt to the needs of daily life. We routinely observed that children were upset by the time limits their parents set using Qustodio. Once set, time limits were fairly rigid: parents had to log back into their accounts using a web browser to change them, and children's devices were blocked from going online without notice after their time allowances ran out. All of the settings enforced by Qustodio

---

[6]https://www.qustodio.com/en/help/article/2460855/
[7]https://blog.rakkoon.com/what-is-rakkoon/
[8]https://www.bark.us/

functioned similarly—parents had to log in on a browser to adjust anything, and children didn't know something was forbidden until they tried to perform the blocked action.

Parental controls could improve families' experiences of rule enforcement if they addressed this inflexibility, and below, we propose three design principles for parental control software that address this issue.

First, parental control software should alert children when they are about to engage in an action that will be blocked or when they are approaching a time limit. Qustodio did not warn users when their time was about to run out for the day, and as a result, the user's internet connection might cut out in the middle of a streaming video or some other unexpected moment. If instead the software sent the child an alert that they had five or ten minutes left, or gave a half hour's notice before the device shut off in the evening, children could proactively modify their behavior so they're not interrupted in the middle of an activity. Warnings would also benefit children if they were about to perform an action that would be reported to the parent or blocked, such as visiting a website that the software as identified as age-inappropriate. This again gives children a chance to rethink their decision: did they know the website might be inappropriate before clicking the link? Do they want to continue, knowing their parent will see this in their browsing history? Should this website not be blocked, is this a mistake on the part of the software? Warnings offer children the opportunity to stop and think about their use of digital devices in the moment, rather than relying primarily on parents to actively monitor the child's activity log and address potential issues after they have occurred.

Second, software could enable children to digitally negotiate with their parents about device use rules. Consider the warnings above: if a child receives a "ten minutes remaining" warning from Qustodio, but they think they should have more time that day, Qustodio could close the loop and enable children to send an alert to their parents with a request for more time before their time has run out. These just-in-time requests could help avoid situations where a child can't access a resource (time, websites, or others). Software-enabled negotiation could also moderate the tone of children's requests to parents: as we saw in our study, children often begged, bickered, or shouted in response to parents' restrictions, and parents did not necessarily respond positively. Automated prompts might reduce tension between parents and children around tricky rules discussions. Text messages could support much of this need, but unlike texts, a negotiation platform built in to the software would be able to clearly indicate its purpose and separate software-related information from other requests or communication that takes place between parent and child.

Third, negotiation features described above would be amplified if parental control software routinely included mobile-friendly interfaces for adjusting parenting settings. Qustodio had a cross-platform app but it did not have a mobile interface for changing the software settings, so parents had to access the web interface on their phone in order to change settings when away from a computer. A full-featured mobile app for parents should be standard for any parental control software. Beyond that, however, software designers should consider additional avenues for parents to update settings on mobile. If a parent got a request for more time from their child, for example, an alert on the parent's phone could take the parent straight to the setting needed to adjust that time limit. Most parental control software offers many settings, and streamlining the interaction so parents are delivered to the right toggle, or can press a button or respond to the alert without opening the app.

The three design principles detailed above together create a guide for parental control software that is responsive to both parents and children. Such software offers unique capabilities to parents, but currently, these features are mostly not smart enough to adapt to the changing daily needs of families. That adaptability could be added by designing a system that encourages children to be active in making decisions about their device use and that enables direct communication about and

adjustment to rules.

7.3.3 Implications for Behavior Contracts

Unlike Qustodio, which was a fairly standard example of parental control software with many similar peers, The Smart Talk was a uniquely well-developed example of an online behavior contract. Other contracts that we reviewed were based on simpler web forms or lacked interactive features altogether. Therefore, our observations about The Smart Talk serve as a roadmap for future tools in this space.

Rule Enforcement

Enforcing rules generated by the contract, especially rules about screen time, is one of the most challenging aspects of using a contract. Screen time concerns were as prevalent for families in this condition as in the software condition. We documented above that parents and children bickered over screen time, and suggest that changes to the framing of time limits might alleviate some of this disagreement. However, enforcing a time limit, once set, can't be made easier with such a simple change.

The Smart Talk did not introduce families to new ideas for making sure that household rules are followed. The framing of the contract ensures that families cover a variety of topics, many of which they may never have explicitly addressed before. But once those topics are adjudicated and new rules negotiated, the work of making sure the child behaves in the agreed-upon manner falls to the parent. As discussed in section 7.1 above, enforcing rules is difficult for parents. Any contract that introduces new rules to a family should also include ideas for maintaining behavior, revisiting rules, and managing exceptions to the rules.

As an illustrative example, families can set a daily screen time allowance using The Smart Talk, but policing that daily allowance is left to the parents to figure out. How should a parent or even a child keep an accurate record of how long the child has used their device? Screen time poses an obvious challenge for enforcement, but any rule could be similarly difficult for a family's individual circumstances. Contracts could, in addition to serving as a checklist of important topics for rules, provide guidance for making rules workable in daily life.

Rule Flexibility

The Smart Talk prompted families to think about many rules they might not have explicitly defined without it, but it did not enable families to declare additional rules specific to their needs. The form field nature of many online contracts restricts families from improvising—we saw that families wanted to assign responsibility for some limits to both parent and child, but because the creators of The Smart Talk had not thought the same, users did not have that option.

Behavior contracts are fundamentally premised on the idea that family rules should be agreed to by parents and children, and customization for a specific family's needs can be a large part of that process. Contract platforms, like The Smart Talk, should create space for families to add unique rules. The Smart Talk, in particular, organizes rules into six distinct categories, and one could imagine a section for custom rules within each category so that families' rules can fit into the pre-existing organization. This extra consideration for the individual needs of each family would help a behavior contract be an adaptable tool appropriate for many situations.

7.3.4 Conclusions

In this section, we see that having rules about appropriate behavior, even when those rules are backed by a parenting tool, is not sufficient to overcome the challenges of digital parenting. Both tools gave parents structure, but that structure came with costs: technical shortcomings, rigidly-enforced rules, or insufficiently enforced rules. Parenting tool companies should improve over these findings by building responsive, educational tools that involve active participation from both parents and children. Online behavior contracts should include education and guidance for families in addition to suggesting topics for rules, so that families can consider new techniques that make rules enforceable and consistent for them. In future work, our implications for both tools could be used to evaluate how well existing tools address families' needs and capabilities.

Chapter 8

Conclusions

This thesis investigates parenting decisions related to adolescent online behavior. In Chapter 2, we establish that online safety considerations are a primary reason for parents to make decisions that are potentially invasive of their children's online privacy. In Chapter 3, we categorize parenting strategies and draw distinctions between them, showing that monitoring, a potentially privacy-invasive strategy, is controversial among online safety experts, parents of teens, and teens; communication-based strategies that proactively involve the teenager as well as the parent were more widely accepted. In Chapter 4, we set up the following three chapters by describing a study methodology in which we assigned families to one of three conditions for a period of one month: use a parenting software, use a behavior contract, or be a control. In Chapter 5, we discuss how these families understood the particular concern of cyberbullying and drama. In Chapter 6, we examine whether these conditions differently affected how families perceived online risks. In Chapter 7, we provide an analysis of the usability challenges posed by these tools. As mentioned previously, this thesis constitute a partial analysis (Chapters 5–7) of the final two studies described in Chapter 4, which will be extended in future work.

In this chapter, we further discuss the conclusions from the previous chapters with an eye towards future work. We begin by discussing perceived tradeoffs between teens' privacy and their safety, and the role that parents play in that tradeoff. We then draw from our findings to examine the ways in which current parenting interventions could be improved. Finally, we conclude with a key idea for future work in this area.

8.1 Teen Privacy and Safety Tradeoffs

Teens express a nuanced understanding of digital privacy, even in an era of increased online sharing of personal information and digital device use at younger and younger ages. However, one of the most commonly-cited privacy concern for teenagers remains privacy intrusions from their own parents; parents often say these intrusions are necessary for the safety of their children. From the parents' perspective, teens' online activities are often difficult to regulate without some degree of monitoring and so monitoring becomes part of the family routine. Though many parents we have studied have expressed that they do not want to intrude on their child's private space, they did not feel like they had a realistic alternative to monitoring their childrens' online activities to some degree.

The study described in Chapter 2 establishes the parental view that privacy and safety are often, if not fundamentally, in opposition to each other. In those interviews, even parents who were were largely permissive of their children's online activities described how they would "violate" their

child's privacy if safety was at stake. Parents largely expressed that they understood their children needed privacy; children largely expressed that they understood their parents needed to make sure they were safe. Nonetheless, parents and children often voiced different opinions of what the child could reasonably consider private information. The study was conducted over the winter of 2013–2014 and during that time, the teen participants described the sanctity of text messages. Today, we would expect that to include mobile social media profiles, such as Instagram and Snapchat, as well [10]. Parents, in contrast, largely did not see text messages as private conversations.

This fundamental disconnect over what aspects of a teen's online activity qualified as "private" hints at an important idea: parents and their children often expressed the same values for online behavior, but differed in how they understood that those values should be enforced. Parents tended to want relatively concrete proof, such as a teen's text message or web browser history, that the teen was still behaving appropriately when using the internet or their digital device. Teens tended to feel that these types of proof were too invasive, but were comfortable giving verbal reassurances of their continued appropriate behavior to their parents. Both parents' and teens' ideas of what constituted an acceptable guarantee were reasonable from their own perspective, but these ideas were difficult to reconcile with each other.

These findings set up a basic tension: more safety means less privacy, at least in the minds of these participants. However, it was not clear from these interviews whether monitoring childrens' digital communications was actually an effective way of ensuring their online safety. We followed up on this study with another aimed at understanding parenting strategies more deeply.

The parenting strategies described by experts can be usefully split into two categories: invasive and non-invasive of the teens' privacy. In Chapter 3, we discussed interviews with 16 online safety experts who described the strengths and weaknesses of many types of parenting strategies. Non-invasive strategies based around communication between the parent and child, such as discussing risky behaviors, were supported by all of these experts. However, we heard contradictory opinions of strategies that involved potentially privacy-invasive actions like monitoring a child's online activity. In surveys of parents of teens and teens, we verified that monitoring-based strategies were indeed considered much less acceptable to teens than communication-based strategies.

8.1.1 Can Parental Monitoring Reasonably Guarantee Children's Safety?

A key component of the professionals' support for monitoring-based parenting interventions was that monitoring was possibly the only way to verify a child's behavior. With most teens owning smartphones and spending an hour or more per day online, these experts felt that communication was necessary but not sufficient. In their view, a "good parent" would ensure their child's safety by scanning through the child's browsing or texting history to watch for risky behavior.

Our studies could not test either that: (1) monitoring will, on average, give the parent more information about what the child is doing online than not monitoring, or that (2) this knowledge will end up making the child safer.

However, it is important to keep this information in context: regarding point #1, children deliberately engaging in risky behaviors may know how to circumvent monitoring efforts, so this may apply only to accidental risk exposure or in limited circumstances. Our studies did not investigate childrens' monitoring circumvention methods or how effective they may be, and we also did not examine how parents' awareness of their children's behavior changed after beginning monitoring. On the other hand, our child participants sometimes expressed that they had hidden some of their online activities from their parents, and our own experimentation with monitoring software showed that software alone would not be sufficient to monitor all of the risky behaviors a teen could engage in online.

Similarly, regarding point #2, parents would need to know how to translate their knowledge of children's behavior into effective strategies to keep their children safer than what they could reasonably expect from having had a conversation with their child about online safety that did not invade the child's privacy. Again, testing this point was outside the scope of our studies. What we can reasonably say is that parent and expert participants most often described setting limits on inappropriate behaviors in response to a child's risky or inappropriate actions, but these types of bans are just likely to lead to the child circumventing the parent's future monitoring efforts in order to avoid further consequences.

Given these points, it is difficult to justify that intensive parental monitoring, as described by some of our expert participants in Chapter 3, would be significantly more effective than less-invasive communication strategies. Monitoring might likely lead to an escalation of teens' efforts to circumvent it, and potentially create an atmosphere of distrust between parent and child, leaving the parent possibly knowing less about what their child is doing online. Discussions or education about online safety might not guarantee a child's online safety, but they also do not necessitate the increased costs to children's privacy of monitoring.

8.1.2 Opportunities for Improving Digital Parenting Strategies

The push and pull between teens' privacy and their safety is key to understanding the parenting decisions being made by families. Companies that create products catered to teens and their families need instead to understand teens and their parents as a unit.

As described at the top of this section, families often see children's privacy and safety as a tradeoff: increasing one decreases the other. Following the argument laid out in that section, we see that teens and parents define what is private and what constitutes reasonable assurance of safety differently. So when a parent wants to increase their assurance of their child's safety, they monitor activity that the teen considers private, and when the child seeks to protect the privacy of their digital behavior, they remove the parent's assurances of safety.

Following from this, tools that give parents easier access to monitoring the child's digital communication, social media activity, or browsing history are likely to be perceived negatively by the child being monitored. Further, as laid out in the subsection above, monitoring, and the bans or limitations that may result from it, could prompt the child to circumvent future parental monitoring.

Parenting software could be a less invasive experience for children. This software is often installed on the child's device, but child-facing features are limited [130]. Instead, most software focuses on increasing the parent's knowledge of the child's activities and enabling parents to restrict it. However, software that obscured the exact nature of the child's activity from the parent except in cases of high risk, or that warned the child user before their activity would be visible to their parent and gave the child a chance to re-evaluate their choice, could balance the needs of both parents and children by preserving more of children's privacy and offering similar safety assurances to parents as what software already offers.

Further, it should be noted that effective use of any parenting strategy depends, in part, on parents understanding their children's online activity and the landscape of apps and devices that children are using. All of the strategies discussed in this thesis would be improved if the parents who implemented them were educated about online behavior and safety. We suggest that examining effective parent education methods and necessary knowledge would be important areas for future work.

Additionally, some responsibility for children's online safety lies with the platforms that they use. Parenting tools are largely reactive to a child encountering risk, and at best, serve as proactive

reminders to avoid known risky behaviors. However, unanticipated risks can be best addressed by platforms. As an example, Instagram disallows nudity and employs community moderators to review and remove content found in violation of this policy; Snapchat does not have this rule. Platforms that have child users are responsible for designing an environment that, by default, minimizes the risky situations a child can end up in and especially that works to prevent risks that are least able to be addressed by parents and parenting tools.

8.2   Usability Challenges in Existing Parenting Interventions

Early on in this work, we found that many parenting strategies were received negatively by teens and professionals' perceptions of their usefulness were divided (Chapter 3). By studying two parenting tools in real families over a period of time, we were able to observe the challenges of these tools for ourselves. As discussed in Chapter 7, usability issues were common and, sometimes, debilitating. The families in our study were invested in learning to use these tools, but even that was not enough to overcome some confusion as early as the setup process.

The Smart Talk behavior contract was generally easier for families to set up; the body of the contract was straightforward to navigate. But the discussion between parent and child often broke down when they were prompted to discuss screen time. As with the disagreement discussed in section 8.1, this was a disagreement on specifics rather than general goals. Though parents and children fundamentally agreed that the child should be able to use their phone when they woke up in the morning and should put it away when they went to bed for the evening, families bickered over the exact times of these events, sometimes down to the minute. The contract's choice to focus on particular times resulted in many children pushing for longer windows of time in which they could use their phones every day while parents pushed for shorter windows. A more general measure of time, such as "when the child wakes up," might have helped families avoid bickering over minutes and stay focused on collaborative negotiation.

Qustodio, the parenting software, posed more challenges commensurate with its more robust set of features. Families assigned to use it often missed important notices or settings completely because they were visually de-emphasized in the interface. The software was also unclear about exactly how each setting functioned, leading many parents to wonder what they had just enabled.

These issues are disappointing. In Chapters 5 and 6, we discuss different facets of how these same families understood online risks, and what was clear was that parents and children recognized the potential harms of many forms of risky behavior. Additionally, parents expressed a lower confidence in their own ability to protect their children than did those children. Together, these suggest the important role that a usable, relevant, and effective parenting tool could play in many families. Instead, both tools we tested were confusing to navigate or understand and did not necessarily provide functionality to address families' most pressing concerns in a way that reflected real parent-child dynamics. The risks we discussed in Chapter 6 are mapped to the tools evaluated in-depth in Chapter 7 in Figure 8.1. Though both strategies nominally address 12 out of 21 risks studied, there are notable gaps that neither tool covered: abduction and texting and driving. Further, many of these risks are not sufficiently addressed by the tools even though a feature is present. As noted in section 6.1, content-restriction software has notable failings, and as noted in Chapter 7, enforcing the rules set by the contract is left, without guidance, to the parent.

Parenting interventions can provide the families that use them with a false sense of security. Our work made clear that certain types of concerns, such as screen time and use of particular apps, was of high daily relevance to many families. Despite this, questions and features from both tools often placed similar weight on these concerns as they did less-relevant issues such as stranger
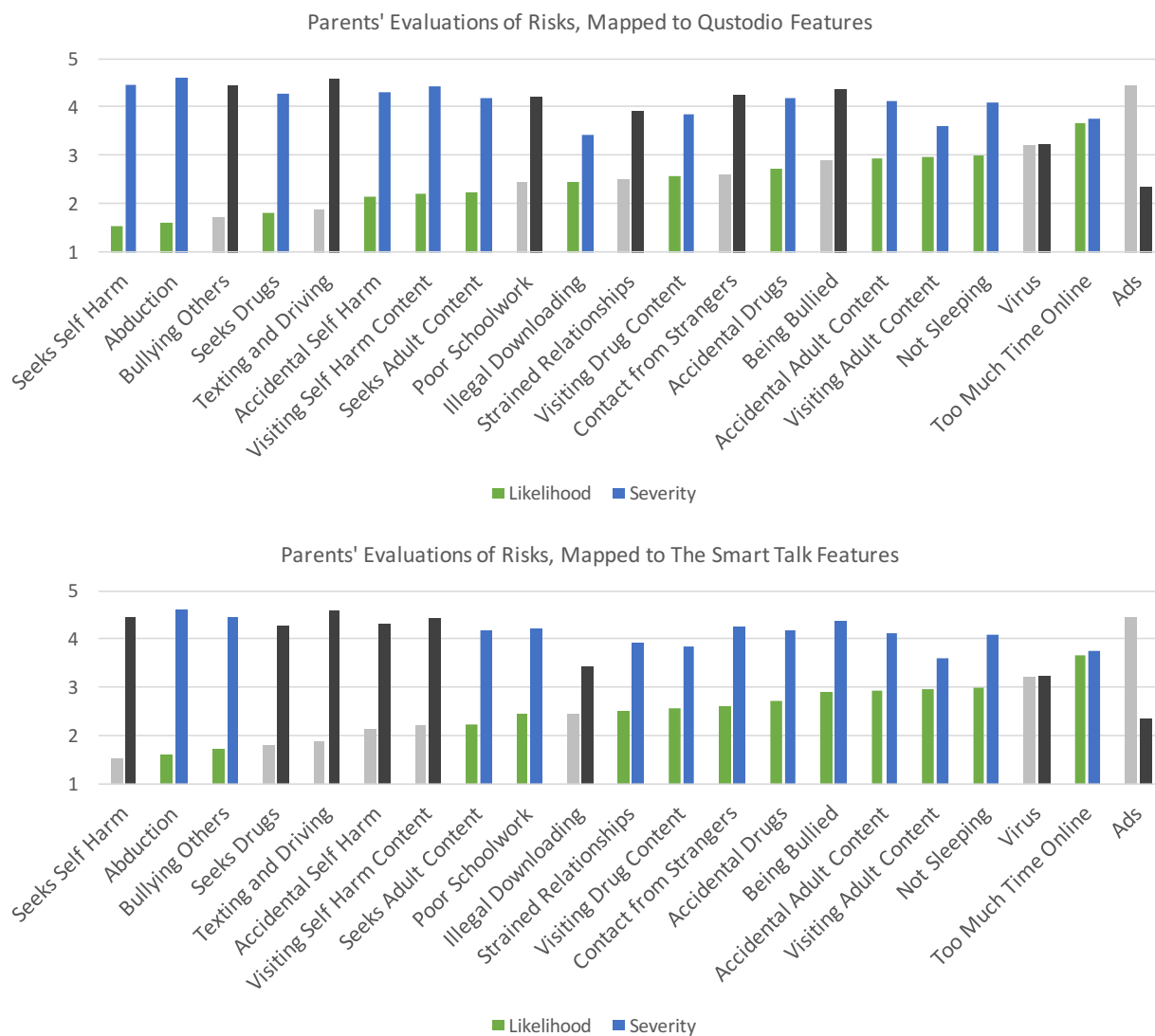
Figure 8.1: These graphs highlight the risks that Qustodio (top panel) and The Smart Talk (bottom panel) offer features to protect against. Risks addressed by the strategy are shown in color. Risks not addressed by the strategy are shown in gray. A strategy was said to have addressed a risk if it mentioned the risk at any point during the configuration process or settings menu.

danger and Facebook use. There is much room for tools and research that will provide guidance for current online safety concerns and the flexibility to adapt to many different family values.

8.3   Limitations

This thesis focused on the perceptions and experiences of digital parenting strategies from both parents and children. As a result of this focus, we do not thoroughly investigate certain populations or types of software.

Child-facing applications, such as social media or gaming apps, are not the subject of the studies in this thesis. However, we suggest that researchers and developers looking at apps or websites with a large number of child users should consider what role the parent may play in that space. We found that parents are one of children's major privacy concerns, and that parents' online safety strategies may impact how the child impacts with a website, app, or device. As a result, websites, apps, and devices that are used by children should anticipate parental involvement when designing for those users.

This thesis also contains a progression from studying parents and children as separate individuals to studying parents and children from the same family unit. Parents have such a substantial role over whether and how the child perceives privacy invasions that studying children's online privacy without hearing from the parent becomes fraught. Specific populations of children, such as those that have a strained relationship with their parent or guardian, and specific topics of interest, such as strictly peer-to-peer privacy concerns, may require or allow for studying children on their own. However, future work in this space must consider, as part of the study design, whether extenuating circumstances require children to be studied independent of their families, and if not, to consider capturing a parent's perspective.

The focus here has been to deepen our understanding of the effects of different parenting strategies on both parents and children. But even in work where the focus is on one of those groups, examining the role that the other might play can help mitigate competing concerns and emphasize cooperation within the family.

8.4   Takeaways for Future Work on Teen Privacy and Digital Parenting

Through the work presented in this thesis, we have learned the unexpected ways in which the interests of parents and their children are inextricably linked. We have seen that parents and children often agree about general values: children should have privacy, parents should get to know their children are safe, children (and parents) should reduce time spent on nonproductive internet browsing. However, we have also seen that parents and children disagree on the specifics of those goals. What this means for technologists and researchers is that if the goal is to study or design for the child user, one must also study or design for the parent so that the specific needs of both are met. Likewise, to study or design for the parent in their role as a parent necessitates considering the child.

Prevailing parental control software typically does not consider the child as a participant, and those that do offer limited features to children. This removes agency from the child as a primary user of the device. We suggest that parental control software might see measurably more use or qualitatively better use if it provided a flexible communication path for the parent and the child to collaboratively manage boundaries for the child's online activity.

Appendix A

Parents' and Teens' Perspectives on Privacy: Study Materials

A.1 Interview Script—Parents

Good {morning/afternoon}. My name is ___ and my colleague's name is ___. We will be moderating your interview today. Can we get you a glass of water or anything else to drink?

To begin, we would like you to review this consent form. It contains important information about today's interview. If you consent to the terms and would like to participate in the study, please sign the form and hand it back to us. [Present consent form]

In this research study, we are interviewing a series of teenagers and a separate series of parents of teenagers to investigate whether teens have a right to privacy, as well as what that means. We are also trying to understand how parents and teenagers make decisions about using new devices, apps, and websites. As part of this study, we will be asking you questions that relate to your relationship with members of your family. You are free to choose not to answer any questions, or to stop the interview at any point if you feel uncomfortable. We greatly value your honest and candid responses.

We would like to make an audio recording of this session. Please note that the members of your family will not listen to this interview recording, and we will not discuss with them what you say during the interview. This recording will only be used for the purposes of this study and will only be accessible to the researchers and transcribers. Do you consent to having this session audio recorded?

Demographics

1. How many people other than you live in your house? What is each person's relationship to you? Do you have any children who don't live with you?

2. How old are your children, and what grades are they in?

Online privacy

1. Where are the computers located in your house? Does your child have his/her own computer?

    (a) Where is your child allowed to use a computer?
    (b) At what age was your child first allowed to use a computer?
    (c) Do you have the password to your child's computer?

111

    (d) Do you use the password to check your child's computer?

    (e) Do you monitor your child's computer use in any other way?

2. Does your child have a phone?

    (a) Is it a smartphone?

    (b) Where is your child allowed to use his/her phone?

    (c) At what age was your child first allowed to have his/her own phone?

    (d) Do you have the password to your child's phone?

    (e) Do you use the password to check your child's phone?

    (f) Do you monitor your child's phone use in any other way?

3. Does your child have a tablet, like an iPad?

    (a) Where is your child allowed to use a tablet?

    (b) At what age was your child first allowed to use a tablet?

    (c) Do you have the password to your child's tablet?

    (d) Do you use the password to check your child's tablet?

    (e) Do you monitor your child's tablet use in any other way?

4. Does your child have a gaming device, like an Xbox or Playstation?

    (a) Where is your child allowed to use a gaming device?

    (b) At what age was your child first allowed to use a gaming device?

    (c) Do you monitor your child's gaming use? How?

5. Does your child have an email address? At what age did they sign up for it? Do you have the password to this email account? Do you monitor this email account any other way?

6. Does your child have a Facebook or other social media account? At what age did they sign up for it? Do you have the password to the account? Do you monitor this account any other way? (Are you friends with them?)

7. Do you feel your restrictions are adequate, too much, or too little? Do you feel your child has the right amount of personal space online? Do you suspect your child has ever tried to hide their online activity from you? What changes, if any, would you consider making to your rules?

New technologies

1. How do you hear about new devices, websites, and apps that teenagers are using these days? What about technologies your children use themselves?

2. How do you decide what rules, policies, and strategies to adopt regarding your teen's use of these devices, websites, and apps?

3. Do you have any concerns about your teen's privacy with new devices, websites, and apps?

4. How do you evaluate the privacy risks of new devices, websites, and apps?

5. Do you think about your teen's privacy online in the same way as privacy in the physical world, or differently?

Privacy at home

1. At home, does your child have their own bedroom? If not, with whom do they share the room?

2. Is your child allowed to keep the door to their room closed? Why or why not?

3. Do you knock before entering your child's room? Why or why not? At what age did you start knocking?

4. Under what circumstances do you consider it appropriate to enter your child's bedroom when they are not there? When is it not appropriate? Are there places within their room that are not appropriate for you to go?

5. Do the bedroom doors in your house have locks? Does your child use the locks? When is it appropriate for them to do so? When is it not appropriate?

6. Do you feel that you give your child enough personal time and space at home? As far as you know, does your child think you give them enough time and space?

Social Privacy

1. What proportion of your child's friends do you feel you know? Would you be surprised if your child has friends you are not aware of?

2. Do you impose any restrictions on your child going out with friends, such as based on time, people, or location? Do you require your child to notify you about where he/she is going, and with whom? Do you suspect your child has ever broken these restrictions?

3. Are there any rules in your family about dating? Do you feel you are aware of your child's romantic or sexual experiences?

4. In general, how well does your child keep you informed about his/her life? Are there things you wish he/she would tell you more about?

5. Do you feel your restrictions are adequate? Do you feel you give your child enough, too much, or just the right amount of space for their own social lives? How do you think your child feels about these restrictions?

Other

1. Is there anything your child wouldn't want you to share with others? What kinds of information about your child, if any, would you not share with immediate family members? Extended family members? Friends?

2. In general, is it ethical for a parent to look through their teenagers' text messages? What about their Facebook? Email? Are there any circumstances under which your answer would change?

    - Do teenagers have the right not to reveal information to a parent?

- Do teenagers have the right not to tell their parents about their grades in school?
- Do teenagers have the right not to tell their parents about health information?
- In general, do you think that teenagers have a right to privacy from their parents?
- Do you feel that you respect your child's privacy at home?
- Are there any other privacy rights which a teenager should or should not have from parents that we have not discussed today?
- When you were your son's/daughter's age, did you feel that your parents respected your privacy? Why or why not?
- Do you feel your view of teen privacy is different from how your parents viewed it when you were a teenager?

3. Do you have any other comments or questions about any topics we covered today?

Thank you very much for your participation! Your feedback has been valuable to our research. [Compensate participant]

A.2 Interview Script—Children

Good {morning/afternoon}. My name is ____ and my colleague's name is ____. We will be moderating your interview today. Can we get you a glass of water or anything else to drink?

To begin, we would like you and your parent to review this consent form. It contains important information about today's interview. If you and your parent consent to the terms and would like to participate in the study, please sign the form and hand it back to us. [Present consent form]

At this point, we would like to ask your parent to leave. [Addressing parent] Our interview will take approximately one hour. You are welcome to wait outside or return once we are done. [Wait for parent to leave before continuing].

In this research study, we are interviewing a series of teenagers and a separate series of parents of teenagers to understand whether teens have a right to privacy, as well as what that means. We are also trying to understand how parents and teenagers make decisions about using new devices, apps, and websites. As part of this study, we will be asking you questions that relate to your relationship with members of your family. You are free to choose not to answer any questions, or to stop the interview at any point if you feel uncomfortable. We greatly value your honest and candid responses.

We would like to make an audio recording of this session. The members of your family will not listen to this interview recording, and we will not discuss with them what you say during the interview. This recording will only be used for the purposes of this study and will only be accessible to the researchers. Do you consent to having this session audio recorded?

Demographics

1. How old are you?

2. How many people other than you live in your house? What is each person's relationship to you?

3. What grade are you in school?

Online privacy

1. Do you have a computer? Where are the computers located in your house?

    (a) Where are you allowed to use your computer?
    (b) At what age were you first allowed to use a computer?
    (c) Do your parents have the password to your computer?
    (d) Do your parents use the password to check your computer?
    (e) Do your parents monitor your computer use in any other way?

2. Do you have a phone?

    (a) Is it a smartphone?
    (b) Where are you allowed to use your phone?
    (c) At what age were you first allowed to use a phone?
    (d) Do your parents have the password to your phone?
    (e) Do your parents use the password to check your phone?
    (f) Do your parents monitor your phone use in any other way?

3. Do you have a tablet?

    (a) Where are you allowed to use a tablet?
    (b) At what age were you first allowed to use a tablet?
    (c) Do your parents have the password to your tablet?
    (d) Do your parents use the password to check your tablet?
    (e) Do your parents monitor your tablet use in any other way?

4. Do you have a gaming device, like an Xbox or Playstation?

    (a) Where are you allowed to use a game console?
    (b) At what age were you first allowed to use a game console?
    (c) Do your parents monitor your game console use?

5. Do you have an email address? At what age did you sign up for it? Do your parents have the password to this email account? Do your parents monitor your email account in any other way?

6. Do you have a Facebook, Instagram, Twitter, or other social media account? At what age did you sign up for it? Do your parents have the password to this account? Do your parents monitor this account any other way?

7. Do you feel your parents' restrictions are adequate, too much, or too little? Do you feel your parents respect your privacy online? Have you ever tried to get around their restrictions? What changes, if any, would you make to your parents' rules?

Space and New Technologies

1. What do you consider to be **your** space online, where you feel comfortable? What parts, if any, would you be comfortable with your parents seeing? Ideally, what would be your space online?

2. What devices do you own that you would consider your space?

3. What does it mean for something to be your space?

4. Do you look at things online that you wouldn't want your parents to know about? Do you think that your parents might know anyway?

5. How do you hear about new websites and apps?

6. How do you decide whether to join or use these new sites and apps?

7. Do you consider privacy when joining or using them? If so, how do you evaluate the privacy risks?

8. Do you think about your privacy online in the same way as privacy in the physical world, or differently?

9. Do you think your parents understand your privacy needs? Do you think your parents understand what it's like to grow up today, and how it differs from when they grew up?

Privacy at home

1. At home, do you have your own bedroom? If not, with whom do you share your room?

2. Are you allowed to keep the door to your room closed? Why or why not?

3. Do your parents knock before entering your room? Why or why not? At what age did they start knocking?

4. Under what circumstances do you consider it appropriate for your parents to enter your room when you are not there? When is it not appropriate? Are there places within your room that are not appropriate for them to go?

5. Do the bedroom doors in your house have locks? Do you use these locks? If so, when do you use it? Why? Is it appropriate for your parents to unlock your door?

6. Do you feel that your parents give you enough personal time and space at home? As far as you know, do they think they give you enough time and space?

Social privacy

1. What proportion of your friends do your parents know? Do you think you should have to tell your parents about all of your friends?

2. Do your parents impose any restrictions on you going out with friends, such as based on time, people, or location? Do they require you to notify them about where you are going, and with whom? Have you ever broken these restrictions?

3. Are there any rules in your family about dating? In general, are your parents aware of your romantic or sexual experiences?

4. Do your parents give you too little, too much, or just the right amount of space for your social life? How do you feel about these restrictions?

Other

1. Are you aware of any laws relating to children and privacy? What laws do you think there should be?

2. (Optional) Should existing privacy laws be removed or changed?

3. What kinds of information about you, if any, would you not want your parents to share with others? (e.g. family)

4. In general, is it ethical for a parent to look through their teenagers' text messages, Facebook, or email? Are there any circumstances under which your answer would change?

   - Do teenagers have the right not to reveal information to a parent?
   - Do teenagers have the right not to tell their parents about their grades in school?
   - Do teenagers have the right not to tell their parents about health information?
   - In general, do you think that teenagers have a right to privacy from their parents?
   - Do you feel that your parents respect your privacy at home?
   - Are there any other privacy rights which a teenager should or should not have from parents that we have not discussed today?

5. Do you think your siblings' answers to the questions today would have been similar to or different from yours?

6. Do you think your parents would be surprised to hear any of your responses today?

7. Do you have any other comments or questions about any topics we covered today?

Thank you very much for your participation! Your feedback has been valuable to our research. We will eventually write a research paper about the conversations we have had with you and other research participants. In the paper, we would like to include quotations from some of our participants with attribution in the form of "Participant #." Do you give us permission to use excerpts from this interview in this research paper? Is there anything that we discussed today which you would like us not to quote? Thanks again! [Compensate participant]

Appendix B

Digital Parenting: A Comparative View of Strategies: Study Materials

B.1 Expert Interview Script

Good morning/good afternoon, my name is _____, and my colleague's name is _____. We will be moderating your interview today.

To begin, we would like you to review the consent form. It contains important information about today's interview. If you consent to the terms and would like to participate in the study, please say, "I consent to participating in this study."

In this study, we are interviewing a series of experts in teen behavior, online safety, privacy, security, and related fields. The purpose of the study is to understand the risks to teens who actively engage online, the efficacy of parents' efforts to mitigate that risk through monitoring and restriction their teens' activities, and what role third parties, including law enforcement officers, educators, and software tools, should play in reducing teens risky online behavior.

During this interview, we may ask some questions that seem to have obvious answers. We just want to make sure we don't miss anything, so even if the answer seems obvious, we appreciate you taking the time to respond fully. You are free to choose not to answer any questions, or to stop the interview at any point if you feel uncomfortable. We greatly value your honest and candid responses.

We would like to make an audio recording of this session. This recording will only be used for the purposes of this study and will only be accessible to the researchers. Do you consent to having this session audio recorded?

Teens' online behaviors

- How are teens using the internet in their free time (that is, not for work)?

- In general, who are teens communicating with online?

- What do you consider a normal use pattern for teens engaging online? Abnormal?

- If a teen is talking to their local peer group:

    - what types of websites or applications do they use?
    - what do they talk about?
    - what are the common safety risks?

- how are teens benefitting from this?

- If a teen is talking to people they do not know in real life:

  - what types of websites or applications do they use?
  - what do they talk about?
  - what are the common safety risks?
  - how are teens benefitting from this?

Risks and harms

Throughout this section, if interviewee is not clear as to why a risk is bad, prompt them for why it is bad.

I'm now going to ask you some questions about risks, by which we mean potential negative outcomes in a given scenario.

- What are some common risks to teens engaging with others online?

- What are the risks associated with:

  - communicating with peers? (see above)
  - communicating with strangers? (see above)
  - using a mobile phone

- How do risks change by:

  - website/service?
  - device (pc versus mobile)?
  - access to peripherals (cameras, microphones, anything else?)?

The following two questions are only necessary if the interviewee has not explained why the risks of the previous questions are negative.

- What long-term negative consequences can result from the risks already described?

- What do you perceive as the most commonly experienced negative consequences?

- How would you address or prevent these problems?

  - From your own expert perspective, that is, as a researcher/law enforcement officer/etc.
  - How could parents address or prevent these problems? If you are a parent, how would you address this?
  - From the perspective of a concerned adult mentor (teacher, counselor, group leader, etc.)?

Effective restrictions and rule enforcement

- Are there any rules that parents make for their own kids that you think would be helpful in addressing potential risks or negative consequences of teens' online behavior?

    – Which of these would a teen respond well to?

- Teens don't always respond well to their parents' rules. Are there any rules to which you think a teen might respond poorly?

- What do you think would be the best approach for developing a rule to which teens would respond well?

- Are there any areas where you do not believe restrictions are the most beneficial method of guiding teens' online behavior? If so, what are they?

- Which of these rules should parents use software tools to enforce?

- If a child violates a parent's restrictions, what do you think should be the consequence for that violation?

Parental practices

- Are there any parental practices regarding teens' online behavior that you believe are effective? If so, what are they?

- Are there any parental practices regarding teens' online behavior that you believe are misguided or ineffective? If so, what are they?

Other stakeholders

- Besides parents, who else is responsible for keeping kids safe? What should they be doing?

    – What role do you think schools, police, service providers, etc. should take?

- Should there be laws to address this? What should they regulate?

Software

- If there was a software tool to address teens' online safety, what should it do?

Closing questions

- Do you have any final thoughts, or questions you would like to ask us?

- How would you like to be identified in any research papers resulting from this study? For example, [customized for each participant], "an executive director of a child-advocacy nonprofit."

B.2 Parent and Teen Survey Script

Demographics

The questions below ask for some basic information about you.

- How old are you?

- Are you the parent or guardian of a teenager?

  - Yes
  - No
  - Prefer not to answer

- What is your sex or gender?

  - Male
  - Female
  - Other identification
  - Prefer not to answer

- What is your race? You may select more than one.

  - American Indian or Alaska Native
  - Asian
  - Black or African American
  - Native Hawaiian or other Pacific Islander
  - White
  - Some other race (please specify)
  - Prefer not to answer

- Are you Hispanic or Latino?

  - Yes
  - No
  - Prefer not to answer

- (Parent) How old are your teenaged children?

  - 13
  - 14
  - 15
  - 16
  - 17
  - 18
  - I do not have any teenaged children

On the following pages you will be asked questions about social media, which includes platforms such as Facebook, Instagram, Twitter, Snapchat, Tumblr and other places where people interact online.

Scenarios

Randomly display one of the following scenarios. Possible names: LaToya, Meredith, Brad or Lamar.

$e://Field/name, a high school student, sees a post about $e://Field/selfon social media made by a classmate. The post is making fun of $e://Field/name, and has a lot of likes and comments from other classmates adding on. $e://Field/name's classmate has made a similar post about $e://Field/namealmost every day this week, and $e://Field/namefeels hurt by these posts.

$e://Field/name, a high school student, sees a post about $e://Field/selfon social media made by a friend. The post is making fun of $e://Field/name, and $e://Field/subjectlaughed it off, but wishes the friend would not have made the post.

- Which of the following statements describe what $e://Field/name's $e://Field/perpetratordid? (Check as many as apply.)

  - I have done this kind of thing in the past
  - This kind of thing has happened to me in the past (I have been in $e://Field/name's situation)
  - This kind of behavior is common
  - This kind of behavior is appropriate
  - This is bullying
  - This is typical teen drama
  - This sounds like a fun interaction
  - This reflects poor judgment
  - This kind of behavior is annoying to others
  - Other (please describe)

Additional Questions

Please rate whether you think knowing the following about someone would make $e://Field/target_teen more or less likely to friend someone$e://Field/teen_pronoun did not know personally.

Scale:

- Less likely
- Somewhat less likely
- Neither more nor less likely
- Somewhat more likely
- More likely

Questions:

- This person is a lot older than $e://Field/target_teen.
- This person and $e://Field/target_teen are the same age.

- This person and $e://Field/target_teen both go to the same school.

- This person does not live near $e://Field/target_teen.

- This person has many friends in common with $e://Field/target_teen.

- This person and $e://Field/target_teen have no friends in common.

For each of the following, please indicate whether you think the following are effective or ineffective ways for parents to help their teenaged children stay safe online.
Scale:

- Ineffective

- Somewhat ineffective

- Neither ineffective nor effective

- Somewhat effective

- Effective

Questions:

- Using parental controls and other software tools to monitor what teens are doing online.

- Looking at teens' social media accounts and reading their posts and messages to monitor what teens are doing online.

- Setting time limits on device use, taking away devices as punishment, or otherwise setting rules and limits on how teens can use the Internet.

- Telling teens about how other teenagers' unsafe online actions have had serious consequences for their personal safety to warn against those actions.

- Teaching teens about what online activity they consider appropriate, and how to handle potentially unsafe situations online.

- Discussing online activity and unsafe situations with teens, including back-and-forth questions and sharing experiences.

- Letting teens experience social media on their own, without interjecting additional information or oversight.

For these same techniques, how acceptable would a teen find it if parent used each of the following to help their teenaged children stay safe online?
Scale:

- Unacceptable

- Somewhat unacceptable

- Neither unacceptable nor acceptable

124

- Somewhat acceptable

- Acceptable

Questions:

- Using parental controls and other software tools to monitor what teens are doing online.

- Looking at teens' social media accounts and reading their posts and messages to monitor what teens are doing online.

- Setting time limits on device use, taking away devices as punishment, or otherwise setting rules and limits on how teens can use the Internet.

- Telling teens about how other teenagers' unsafe online actions have had serious consequences for their personal safety to warn against those actions.

- Teaching teens about what online activity they consider appropriate, and how to handle potentially unsafe situations online.

- Discussing online activity and unsafe situations with teens, including back-and-forth questions and sharing experiences.

- Letting teens experience social media on their own, without interjecting additional information or oversight.

- (Parent) Briefly describe the most effective method you have personally used to keep your teen safe online.

- (Parent) Which of the previous seven categories best describe your method? Check as many as apply.

  - Using parental controls and other software tools to monitor what teens are doing online.
  - Looking at teens' social media accounts and reading their posts and messages to monitor what teens are doing online.
  - Setting time limits on device use, taking away devices as punishment, or otherwise setting rules and limits on how teens can use the Internet.
  - Telling teens about how other teenagers' unsafe online actions have had serious consequences for their personal safety to warn against those actions.
  - Teaching teens about what online activity they consider appropriate, and how to handle potentially unsafe situations online.
  - Discussing online activity and unsafe situations with teens, including back-and-forth questions and sharing experiences.
  - Letting teens experience social media on their own, without interjecting additional information or oversight.

- (Parent) How effective was your method at keeping your teen safe online?

  - Ineffective
  - Somewhat ineffective

- Neither ineffective nor effective
- Somewhat effective
- Effective

• (Parent) How acceptable to your teen was your method of keeping them safe online?

- Unacceptable
- Somewhat unacceptable
- Neither unacceptable nor acceptable
- Somewhat acceptable
- Acceptable

• (Teen) How much ofyour online activity do you try to hide fromyour parents?

- None
- A little
- A lot
- Most
- All

• (Parent) How much of their online activity do you think your teenager tries to hide from you?

- None
- A little
- A lot
- Most
- All

• How important do you think it is to$e://Field/target_teento be able to keep some of$e://Field/teen_possessive mediaactivity private from$e://Field/target_parent?

- Unimportant
- Somewhat unimportant
- Neither unimportant nor important
- Somewhat important
- Important

Appendix C

Longitudinal Interview Study of Parenting Strategies: Materials

C.1 Entrance Interview Script: Parent

I'm going to start recording our interview now. Is it okay with you that I make an audio recording? [Begin recording now]

- Why did you choose to buy your child a phone?

- What does your child do with their smartphone?

- How many hours a day do you think your child uses their phone?

[**Section** – **What is appropriate behavior**]

- What do you hope they will do with their phone?

- What are some examples of activities you want your child to do with their device / online access?

    – Examples of content you want your child to view online?

- What are some examples of activities you do not want your child to do with their device / access online? Content you do not want your child to view online?

- What times, if any, are inappropriate for your child to use their device?

- Do you allow your child to keep their phone in their room overnight?

- What level of oversight over your child's digital activities do you think is necessary / appropriate for you as a parent?

- Is there anything on you child's phone that you know they consider private? What? Do you respect their desire for privacy?

- Are there any areas where you would not want to have oversight / want to give them more space?

- What amount of personal space do you think is necessary / appropriate for your child?

[**Section – Cyberbullying questions**]

I am going to show you two short stories about teens interacting online and ask you some questions about them.

[Note to interviewershow card with name that corresponds to child's gender.]

[Also give parent response card for first scenario]

[Randomly select which of the two scenarios is shown first.]

[Jennifer / Michael], a high school student, sees a post about [herself / himself] on social media made by a friend. The post is making fun of [Jennifer / Michael], and [she / he] laughed it off, but wishes the friend would not have made the post.

[Jennifer / Michael], a high school student, sees a post about [herself / himself] on social media made by a classmate. The post is making fun of [Jennifer / Michael], and has a lot of likes and comments from other classmates adding on. [Jennifer / Michael]'s classmate has made a similar post about [Jennifer / Michael] almost every day this week, and [Jennifer / Michael] feels hurt by these posts.

[First scenario only]

Okay, now that you've read that, I want you to mark whether you agree with any of the follow statements describing this interaction. [Hand card] You may check as many statements as you think apply.

[Do for each scenario separately]

- What do you think about what Jennifer/Michael's peer (classmate, friend, depending on scenario) did, do you think it was ok?

- Would you call this bullying, or more like just teen drama? Why?

[After scenarios are finished]

- How do these scenarios feel different to you?

- What is cyberbullying? What do you consider to be cyberbullying?

- What is teen drama? What do you consider to be just drama between teens?

- Can you imagine any sort of cyberbullying incident that your child or your child's friends might have come across, or could be involved in?

[**Section – Concerns about behavior**]

- You hear about all sorts of online safety risks—What online safety risks to your child worry you personally?

- How likely are those risks?

- How bad would it be if this happened?

Prompt participant with each of the following, if not already mentioned:

- contact by strangers

- abduction

- self-harm, including eating disorders

- cyberbullying

- adult content

- drugs / alcohol

- illegal downloading / filesharing / illegally streaming movies

- lack of sleep

- suffering schoolwork

- offline social impact (family / friends)

- texting while driving

- Are your concerns about online risks any different when your child uses a desktop or laptop computer, versus a smartphone?

- How confident are you in your ability to protect your child from online risks? With whatever tools you have at your disposal right now. Current ability.

- What strategies have you used in the past to keep your child safe online? [Prompt parents with the following list after first answer.]

  - Software monitoring: Have you used any special tools to monitor your child online?
  - Nontechnical monitoring: Have you monitored your child in any other way?
  - Limits: Have you put in place any rules about your child's online activity?
  - Fear appeal: Have you ever told your child stories of consequences other children have experienced as a result of what they were doing online?
  - Education: Have you ever taught your child about appropriate digital behavior?
  - Discussion: Have you ever had a back-and-forth discussion with your child about their online behavior?
  - Complacency: Is there anything your child does online that you've chosen not to engage with, or aren't sure how to engage with?
  - Also note if they say something that doesn't feel like it fits in any of the above!

[**Final questions**]

- What kinds of conflicts have you had with your child about their use of their phone or computer? What prompts those conflicts?

  - What was the outcome of that conflict?
  - What would you do differently next time?
  - What satisfied you about the outcome?

[End recording]

[Section – Survey]

We are going to have you fill out a survey on the topics we just discussed. Please let us know if you have any questions or need anything while you are completing the survey.

(see separate survey documentation)

[Section – Tool Setup]

Now, we're going to have you rejoin your child in the lab.

[Participants will be randomly selected into one of three conditions.]

[Condition One – Control]

- Could you both tell me about your household rules that apply to [child]'s online behavior?

(these participants go straight to compensation and exit)

[Condition Two – Contract]

Okay, we're going to have you visit a website where you create a family internet contract. Once on the page, click "Get me started" to begin.

Site URL: https://thesmarttalk.org/

As you complete the contract, please discuss aloud your thoughts about each question and your responses to them. Please make sure to explain how you both arrive at a decision, even for questions where you immediately agree on an answer.

[Condition Three – Software]

Okay, we're going to have you, [parent], visit a website on a computer. On this website, you will create an account for a parenting software. We will provide you [the parent] with a password for this account; please use this password when you register for Qustodio.

We will also have you install the app for this software on [child]'s phone. Once [parent] has created the account, [parent] will receive an email instructing them to set up the software on the child's phone.

As you are completing these tasks, please discuss aloud what you are thinking about the process.

Okay, now that the software is installed, we would like [parent] to configure the settings for this software. Please discuss aloud what settings you are choosing, and why you are choosing them.

Once you have completed setting up this software, please take screenshots of the software settings. We will reference these again after one month has gone by.

[Section – Exit]

Thank you for coming in to the lab today to participate in our study. Do you have any remaining questions for us?

We will send you remaining a short survey each week so that you can report your experiences together over the next month. We will also schedule a follow-up interview for one month from now. If you know your availability, we can schedule that now, or we will send you a reminder with each weekly survey.

130

C.2   Entrance Interview Script: Child

I'm going to start recording our interview now. Is it okay with you that I make an audio recording?
[Begin recording now]

- Why did you you want to get a smartphone?

- How did you get your smartphone? e.g. Was it a gift? Your parent's old phone? Have you had multiple phones?

- How many hours a day do you think you use your phone?

[**Section – What is appropriate behavior**]

- What do you use your phone for now? Is there anything else you would like to use

- your phone for?

- What are some examples of activities you do or apps that you use? Can you show me?

- What are some examples of activities or apps that you would not use?

- What times, if any, are inappropriate for you to use your phone?

  - Do you use your phone then anyway?
  - Are you allowed to keep your phone in your room overnight?

- Do you think your parents should check to see what you are using your phone for or who you are communicating with?

  - What types of devices or applications do you think they should check?
  - Why do you think they should check this?
  - Is there anything you don't think they should check? Why?

- Is there anything on your phone that you consider private?

  - What is it?
  - Why do you consider it private?
  - Do your parents respect your desire for privacy in this case?

[**Section – Cyberbullying questions**]

I am going to show you two short stories about teens interacting online and ask you some questions about them.
[Note to interviewershow card with name that corresponds to child's own gender.]
[Also give child response card for first scenario]
[Randomly select which of the two scenarios is shown first.]
[Jennifer / Michael], a high school student, sees a post about [herself / himself] on social media made by a friend. The post is making fun of [Jennifer / Michael], and [she / he] laughed it off, but wishes the friend would not have made the post.

[Jennifer / Michael], a high school student, sees a post about [herself / himself] on social media made by a classmate. The post is making fun of [Jennifer / Michael], and has a lot of likes and comments from other classmates adding on. [Jennifer / Michael]'s classmate has made a similar post about [Jennifer / Michael] almost every day this week, and [Jennifer / Michael] feels hurt by these posts.

[First scenario only]

Okay, now that you've read that, I want you to mark whether you agree with any of the follow statements describing this interaction. [Hand card] You may check as many statements as you think apply.

[Do for each scenario separately]

- What do you think about what Jennifer/Michael's peer (classmate, friend, depending on scenario) did, do you think it was ok?

- Would you call this bullying, or more like just teen drama? Why?

[After scenarios are finished]

- How do these scenarios feel different to you?

- What is cyberbullying? What do you consider to be cyberbullying?

- What is teen drama? What do you consider to be just drama between teens?

- Can you imagine any sort of cyberbullying incident that you or your friends might have come across, or could be involved in?

[Section – Concerns about online risks]

- You hear about all sorts of online safety risks—What online safety risks to *you* worry you?

- How likely are those risks?

- How bad would it be if this happened?

Prompt participant with each of the following, if not already mentioned:

- contact by strangers

- abduction

- self-harm, including eating disorders

- cyberbullying

- adult content

- drugs / alcohol

- illegal downloading / filesharing

- viruses / malware

- lack of sleep

132

- suffering schoolwork

- offline social impact (family / friends)

- texting while driving

- Are your concerns about online risks any different when you use a desktop or laptop computer, versus a smartphone?

- How confident are you in your ability to protect yourself from online risks? With whatever tools you have at your disposal right now. Current ability.

- How confident are you that your parent can protect you from online risks?

- What strategies have you used in the past to keep yourself safe online?

- What strategies have your parents used in the past to keep you safe online?

[Final questions]

- What kinds of conflicts have you had with your parent about using your phone or computer? What prompts those conflicts?

    - What was the outcome of that conflict?
    - What would you do differently next time?
    - What satisfied you about the outcome?

[Section – Survey]

We are going to have you fill out a survey on the topics we just discussed. Please let us know if you have any questions or need anything while you are completing the survey.

(see separate survey documentation)

[Section – Tool Setup]

Now, we're going to have you rejoin your child in the lab.

[Participants will be randomly selected into one of three conditions.]

[Condition One – Control]

- Could you both tell me about your household rules that apply to [child]'s online behavior?

(these participants go straight to compensation and exit)

[Condition Two – Contract]

Okay, we're going to have you visit a website where you create a family internet contract. Once on the page, click "Get me started" to begin.

Site URL: https://thesmarttalk.org/

As you complete the contract, please discuss aloud your thoughts about each question and your responses to them. Please make sure to explain how you both arrive at a decision, even for questions where you immediately agree on an answer.

[Condition Three – Software]

Okay, we're going to have you, [parent], visit a website on a computer. On this website, you will create an account for a parenting software. We will provide you [the parent] with a password for this account; please use this password when you register for Qustodio.

We will also have you install the app for this software on [child]'s phone. Once [parent] has created the account, [parent] will receive an email instructing them to set up the software on the child's phone.

As you are completing these tasks, please discuss aloud what you are thinking about the process.

Okay, now that the software is installed, we would like [parent] to configure the settings for this software. Please discuss aloud what settings you are choosing, and why you are choosing them.

Once you have completed setting up this software, please take screenshots of the software settings. We will reference these again after one month has gone by.

[Section – Exit]

Thank you for coming in to the lab today to participate in our study. Do you have any remaining questions for us?

We will send you remaining a short survey each week so that you can report your experiences together over the next month. We will also schedule a follow-up interview for one month from now. If you know your availability, we can schedule that now, or we will send you a reminder with each weekly survey.

[End recording]

C.3   Entrance Survey: Parent

Demographics

The questions below ask for some basic information about you.

- How old are you?

- What is your sex or gender?

    - Male

    - Female

    - Other identification

    - Prefer not to answer

- Are you the parent or guardian of a teenager?

    - Yes

    - No

    - Prefer not to answer

- What is your race? You may select more than one.

    - American Indian or Alaska Native

    - Asian

- Black or African American
- Native Hawaiian or other Pacific Islander
- White
- Some other race (please specify)
- Prefer not to answer

- Are you Hispanic or Latino?

  - Yes
  - No
  - Prefer not to answer

- How old are your teenaged children?

  - 13
  - 14
  - 15
  - 16
  - 17
  - 18
  - I do not have any teenaged children

- What is the birthdate of your child who will also be taking part in this study?

- What type of school does your child attend?

  - Public
  - Private
  - Charter
  - Home school

- How many students are enrolled at your child's school?

  - 500 or fewer
  - 501 - 1000
  - 1001 - 1500
  - 1501 - 2000
  - 2001 - 2500
  - 2501 - 3000
  - More than 3000 students

- What is the grade range of your child's school? For example, a typical four-year high school would be grades 9 - 12, and a school that combines kindergarten through eighth grade students would be K - 8.

- What is the highest level of education you have received?

- Less than high school degree
- High school degree or equivalent (e.g., GED)
- Some college but no degree
- Associate degree
- Bachelor degree
- Graduate degree

• What is your household income?

- Less than $20,000
- $20,000 to $34,999
- $35,000 to $49,999
- $50,000 to $74,999
- $75,000 to $99,999
- $100,000 to $149,999
- $150,000 to $199,999
- $200,000 or more

• What is your marital status?

- Widowed
- Divorced
- Separated
- Married
- Never married

On the following pages you will be asked questions about social media, which includes platforms such as Facebook, Instagram, Twitter, Snapchat, Tumblr and other places where people interact online.

You will also periodically be asked questions that refer to "your child," which here indicates the child with whom you are participating in this study.

• Why did you choose to get your child a smartphone?

• What online safety risks to your child worry you?

Online Risks

Please rate each of the following online risks for how likely they are, their level of severity, and how confident you are in your ability to protect your child from them.
Question:

• How bad would it be if the your child experienced the following?

Scale: Not at all bad – Extremely bad
Risks:

- Bullying another person online

- Being bullied online by another person

- Visiting sites with sexual or other adult content

- Visiting sites that urge them to use drugs or alcohol

- Visiting websites that urge them to harm themself

- Illegally downloading copyrighted material, like music

- Getting a virus on their phone, tablet, or computer

- Texting or talking on the phone while driving

- Not getting enough sleep because of spending too much time online

- Doing poorly in school because of spending too much time online

- Having trouble with friends or family because of spending too much time online

- Being contacted by a stranger

- Being abducted by a stranger you met online

Question:

- How likely is your child to experience each of the following?

Scale: Very unlikely – Very likely
Risks as above
Question:

- How confident are you that you would be able to prevent each of the following from happening to your child?

Scale: Not at all confident – Extremely confident
Risks as above

Parenting Strategies

- Briefly describe something you have done or are currently doing to protect your child from online risks.

- Which of the following categories best describes your method? Check all that apply.

  - Using parental controls and other software tools to monitor what your child is doing online.
  - Looking at your child's social media accounts and reading their posts and messages to monitor what they are doing online.
  - Setting time limits on device use, taking away devices as punishment, or otherwise setting rules and limits on how your child can use the Internet.

137

– Telling your child about how other teenagers' unsafe online actions have had serious consequences for their personal safety to warn against those actions.

– Teaching your child about what online activity you consider appropriate, and how to handle potentially unsafe situations online.

– Discussing online activity and unsafe situations with your child, including back-and-forth questions and sharing experiences.

– Letting your child experience social media on their own, without interjecting additional information or oversight.

– Other

Please indicate how frequently you use each of the following parenting strategies.

• Using parental controls and other software tools to monitor what your child is doing online.

– This is a primary strategy for me

– This is a secondary strategy for me

– I occasionally use this strategy

– I do not use this strategy

• Please briefly describe how you use this strategy.

• Looking at your child's social media accounts and reading their posts and messages to monitor what they are doing online.

– This is a primary strategy for me

– This is a secondary strategy for me

– I occasionally use this strategy

– I do not use this strategy

• Please briefly describe how you use this strategy.

• Setting time limits on device use, taking away devices as punishment, or otherwise setting rules and limits on how your child can use the Internet.

– This is a primary strategy for me

– This is a secondary strategy for me

– I occasionally use this strategy

– I do not use this strategy

• Please briefly describe how you use this strategy.

• Telling your child about how other teenagers' unsafe online actions have had serious consequences for their personal safety to warn against those actions.

– This is a primary strategy for me

– This is a secondary strategy for me

– I occasionally use this strategy

      – I do not use this strategy

- Please briefly describe how you use this strategy.

- Teaching your child about what online activity you consider appropriate, and how to handle potentially unsafe situations online.

      – This is a primary strategy for me

      – This is a secondary strategy for me

      – I occasionally use this strategy

      – I do not use this strategy

- Please briefly describe how you use this strategy.

- Discussing online activity and unsafe situations with your child, including back-and-forth questions and sharing experiences.

      – This is a primary strategy for me

      – This is a secondary strategy for me

      – I occasionally use this strategy

      – I do not use this strategy

- Please briefly describe how you use this strategy.

- Letting your child experience social media on their own, without interjecting additional information or oversight.

      – This is a primary strategy for me

      – This is a secondary strategy for me

      – I occasionally use this strategy

      – I do not use this strategy

- Please briefly describe how you use this strategy.

- Are there any other adults in your household or in your child's life who employ parenting strategies to keep your child safe online?

      – Yes

      – No

- Briefly describe who these adults are and what strategies they are using to keep your child safe online.

- Please indicate, on average, how frequently you do the following activities in a typical month.

Scale:

- More than once a day

- Between once a day and once a week

- Between once a week and once a month

- Less than once a month

Activities:

- Check your child's personal message history

- Check your child's social media profiles

- Take away your child's smartphone

- Take away your child's personal computer

- Remove smartphone from your child's room overnight

- Discuss online safety with your child

- Discuss news about online behavior with your child

C.4 Entrance Survey: Child

Demographics

The questions below ask for some basic information about you.

- What is your birthdate?

    - Month
    - Day
    - Year

- What is your sex or gender?

    - Male
    - Female
    - Other identification
    - Prefer not to answer

- What is your email address?

On the following pages you will be asked questions about social media, which includes platforms such as Facebook, Instagram, Twitter, Snapchat, Tumblr and other places where people interact online.

You should understand that if your responses to this survey indicate you or someone else is at risk of serious harm, we will take the necessary action to report this to authorities, such as law enforcement. This may include reporting your personal information, including name or address. For example, we will report any cases of child abuse.

- Why did you want to get a smartphone?

- What unsafe things online worry you?

Online Risks

Please rate each of the following online risks for how likely they are, their level of severity, and how confident you are in your ability to protect yourself from them.

- How bad would it be if the you experienced the following?

Scale: Not at all bad – Extremely bad
Risks:

- Bullying another person online

- Being bullied online by another person

- Visiting sites with sexual or other adult content

- Visiting sites that urge you to use drugs or alcohol

- Visiting websites that urge you to harm yourself

- Illegally downloading copyrighted material, like music

- Getting a virus on your phone, tablet, or computer

- Texting or talking on the phone while driving

- Not getting enough sleep because of spending too much time online

- Doing poorly in school because of spending too much time online

- Having trouble with friends or family because of spending too much time online

- Being contacted by a stranger

- Being abducted by a stranger you met online

- How likely are you to experience each of the following?

Scale: Very unlikely – Very likely
Risks as above

- How confident are you that you would be able to prevent each of the following?

Scale: Not at all confident – Extremely confident
Risks as above

- How confident are you that your parent would be able to protect you from each of the following?

Scale: Not at all confident – Extremely confident
Risks as above

Parenting Strategies

- Briefly describe something your parent or guardian is currently doing to protect you from online risks.

- Which of the following categories best describes your parent's or guardian's method? Check all that apply.

  - Using parental controls and other software tools to monitor what you are doing online.
  - Looking at your social media accounts and reading your posts and messages to monitor what you are doing online.
  - Setting time limits on device use, taking away devices as punishment, or otherwise setting rules and limits on how you can use the Internet.
  - Telling you about how other teenagers' unsafe online actions have had serious consequences for their personal safety to warn you against those actions.
  - Teaching you about what online activity your parent/guardian consider appropriate, and how to handle potentially unsafe situations online.
  - Discussing online activity and unsafe situations with you, including back-and-forth questions and sharing experiences.
  - Letting you experience social media on your own, without interjecting additional information or oversight.
  - Other

Please indicate, on average, how frequently your parent or guardian does the following activities in a typical month
Scale:

- More than once a day

- Between once a day and once a week

- Between once a week and once a month

- Less than once a month

Activities:

- Check your personal message history

- Check your social media profiles

- Take away your smartphone

- Take away your personal computer

- Remove your smartphone from your room overnight

- Discuss online safety with you

- Discuss news about online behavior with you

C.5 Weekly Survey

On the next pages, we will ask you to report your experiences during the past week. Please provide as much detail as you are comfortable giving.

Discussions or Disagreement About Online Safety

- Have you and $e://Field/subject had any discussions or disagreements about online activity in the past week? For example, have you talked about a news story that mentioned social media? Have you talked with $e://Field/subject about smartphone use?

  – Yes

  – No

- Please describe your interaction in a few sentences

- In your opinion, what caused the interaction?

- How did the interaction resolve?

- Did you use any tools during the course of this interaction? If so, please describe how.

Risky Situations Online

- In the past week, have you experienced or observed any risky situations online that you did not discuss with $e://Field/subject?

  – Yes

  – No

- Please describe the risky situation in a few sentences

- How did the risky situation resolve?

- Why did you choose not to discuss the risky situation with your parent or child?

- Did you use any tools during the time you observed or experienced this risky situation? If so, please describe how.

C.6 Exit Interview Script: Parent

[Variables will be filled out in advance of interview by the researchers, based on responses to the Weekly Check-In Survey. Multiple rounds of this question may be asked if multiple incidents are reported.]

- You reported that [X] happened on [Y] date. Can you tell me a bit about that?

  – In what context did this happen?

  – Did you come to a resolution about [X]? How?

  – Did you use any tool to deal with [X]? How?

  – Are you satisfied with the outcome?

– Would you do anything differently if it were to occur again?

[Use as prompt only if few/no incident reports]

- Can you tell me about any other online experiences in the past month?

  – Has your child encountered any online safety risks? How did you find out?
  – Did you ever indicate that something your child was doing online was not okay with you?

Software Condition

- How was the overall experience of using Qustodio?

- How often did you use Qustodio?

  – Log in?
  – Make changes to settings?

- Did you feel that Qustodio's email notifications were helpful?

- Do you feel that Qustodio is keeping your child safer online?

- Do you feel that Qustodio has improved your relationship with your child?

- How helpful was Qustodio? Was it confusing? Was there anything you couldn't figure out? Is there any feature you would have liked but don't think Qustodio offers?

- Do you think you will continue using Qustodio going forward?

Contract

- How was the overall experience of using the online behavior contract?

- How often did you reference the contract?

  – Make changes to the contract terms? [Pull out contract and have them mark changes on printed copy]
  – Remind your child of contract terms?
  – Please now let us scan the final contract (ONLY if they bring a revised version of the contract)

- Do you feel that the contract is keeping your child safer online?

- Do you feel that contract has improved your relationship with your child?

- How helpful was the contract? Was it confusing? Was there anything that was not useful? Is there a topic you wished it had covered?

- Do you think you will continue using this contract going forward?

Control

- How was your overall experience in the past month?

- Did you employ any different parenting strategies? How did those work out? Do you feel they kept your child safer online?

C.7   Exit Interview Script: Child

[Variables will be filled out in advance of interview by the researchers, based on responses to the Weekly Check-In Survey. Multiple rounds of this question may be asked if multiple incidents are reported.]

- You reported that [X] happened on [Y] date. Can you tell me a bit about that?

  – In what context did this happen?
  – Did you come to a resolution about [X]? How?
  – Did you use any tool to deal with [X]? How?
  – Are you satisfied with the outcome?
  – Would you do anything differently if it were to occur again?

[Use as prompt only if few/no incident reports]

- Can you tell me about any other online experiences you've had in the past month?

  – Have you encountered any online safety risks? Did you discuss this with your parents?
  – Did your parents ever indicate that something you were doing online was not okay with them?

Software Condition

- How was the overall experience of using Qustodio?

- How often did your parent use Qustodio?

  – Log in?
  – Make changes to settings?
  – Please now screen capture the final settings

- Do you feel that Qustodio is keeping you safer online?

- Do you feel that Qustodio has improved your relationship with your parent?

- Have you ever been stopped from doing something on your phone by Qustodio?

  – How often?
  – What were you doing?

- If you could change anything about Qustodio, would you? What?

Contract

- How was the overall experience of using the online behavior contract?

- How often did you reference the contract?

  - Make changes to the contract terms?
  - Parental reminders of contract terms?
  - Please now scan the final contract (ONLY if bring revised contract

- Do you feel that the contract is keeping you safer online?

- Do you feel that contract has improved your relationship with your parent?

- Have you ever stopped doing something online because you remembered your contract?

  - How often?
  - What were you doing?

- If you could change anything about the contract, would you? What?

Control

- How was your overall experience in the past month?

- Did you parent employ any different parenting strategies? How did those work out? Did they make you feel safer?

C.8   Exit Survey: Parent

On the following pages you will be asked questions about social media, which includes platforms such as Facebook, Instagram, Twitter, Snapchat, Tumblr and other places where people interact online.

- What online safety risks to your child worry you?

Discussions or Disagreement About Online Safety

- Have you and your child had any discussions or disagreements about online activity in the past month?For example, have you talked about a news story that mentioned social media? Have you punished your child for something done online? Have you talked about something your child is doing online?

  - Yes
  - No

- Please describe your interaction in a few sentences

- In your opinion, what caused the interaction?

- How did the interaction resolve?

- Did you use any tools during the course of this interaction? If so, please describe how.

Risky Situations Online

- In the past month, have you observed any risky situations online that you did not discuss with your child?

  - Yes
  - No

- Please describe the risky situation in a few sentences

- How did the risky situation resolve?

- Why did you choose not to discuss the risky situation with your parent or child?

- Did you use any tools during the time you observed or experienced this risky situation? If so, please describe how.

Online Risks

Please rate each of the following online risks for how likely they are, their level of severity, and how confident you are in your ability to protect your child from them.
Question:

- How bad would it be if the your child experienced the following?

Scale: Not at all bad – Extremely bad
Risks:

- Bullying another person online

- Being bullied online by another person

- Visiting sites with sexual or other adult content

- Visiting sites that urge them to use drugs or alcohol

- Visiting websites that urge them to harm themself

- Illegally downloading copyrighted material, like music

- Getting a virus on their phone, tablet, or computer

- Texting or talking on the phone while driving

- Not getting enough sleep because of spending too much time online

- Doing poorly in school because of spending too much time online

- Having trouble with friends or family because of spending too much time online

- Being contacted by a stranger

- Being abducted by a stranger you met online

Question:

- How likely is your child to experience each of the following?

Scale: Very unlikely – Very likely
Risks as above
Question:

- How confident are you that you would be able to prevent each of the following from happening to your child?

Scale: Not at all confident – Extremely confident
Risks as above

Parenting Strategies

- Please indicate, on average, how frequently you do the following activities in a typical month.

Scale:

- More than once a day

- Between once a day and once a week

- Between once a week and once a month

- Less than once a month

Activities:

- Check your child's personal message history

- Check your child's social media profiles

- Take away your child's smartphone

- Take away your child's personal computer

- Remove smartphone from your child's room overnight

- Discuss online safety with your child

- Discuss news about online behavior with your child

Software Condition

- How often did you log in to the parent control panel for Qustodio?

  – More than once a day
  – Between once a day and once a week
  – Between once a week and once a month
  – Less than once a month

- How often did you get an alert from Qustodio about your child's online activity?

– More than once a day

  – Between once a day and once a week

  – Between once a week and once a month

  – Less than once a month

- Did you edit the settings for Qustodio during the past month?

  – Yes

  – No

- What settings have you changed?

- Please briefly describe your experience using Qustodio. Was it helpful? Was it confusing?

- Do you feel like using Qustodio is keeping your child safer online? Why or why not?

Contract Condition

- How often did you review the contract you had written?

  – More than once a day

  – Between once a day and once a week

  – Between once a week and once a month

  – Less than once a month

- How often did you remind your child about the terms of your contract?

  – More than once a day

  – Between once a day and once a week

  – Between once a week and once a month

  – Less than once a month

- Have you edited the terms of the contract during the past month?

  – Yes

  – No

- What did you change about the contract?

- Please briefly describe your experience using an online behavior contract. Was it helpful? Was it confusing?

- Do you feel like using an online behavior contract is keeping your child safer online? Why or why not?

Control Condition

- Have you adopted a new parenting strategy for keeping your child safe online in the past month?

  – Yes

  – No

- Please briefly describe your parenting strategy below.

- Which of the following categories best describes your strategy? Check all that apply.

  – Using parental controls and other software tools to monitor what your child is doing online.

  – Looking at you child's social media accounts and reading their posts and messages to monitor what your child is doing online.

  – Setting time limits on device use, taking away devices as punishment, or otherwise setting rules and limits on how your child can use the Internet.

  – Telling your child about how other teenagers' unsafe online actions have had serious consequences for their personal safety to warn against those actions.

  – Teaching your child about what online activity you consider appropriate, and how to handle potentially unsafe situations online.

  – Discussing online activity and unsafe situations with your child, including back-and-forth questions and sharing experiences.

  – Letting your child experience social media on their own, without interjecting additional information or oversight.

  – Other

- Please describe your experience using this strategy. Was it helpful? Was it confusing?

- Do you feel like using this strategy is keeping your child safer online? Why or why not?

C.9   Exit Survey: Child

On the following pages you will be asked questions about social media, which includes platforms such as Facebook, Instagram, Twitter, Snapchat, Tumblr and other places where people interact online.

- What unsafe things online worry you?

Discussions or Disagreement About Online Safety

- Have you and your parent or guardian had any discussions or disagreements about online activity in the past month? For example, have you talked about a news story that mentioned social media? Have you received a punishment for something done online? Have you talked about something you are doing online?

  – Yes

– No

- Please describe your interaction in a few sentences

- In your opinion, what caused the interaction?

- How did the interaction resolve?

- Did you use any tools during the course of this interaction? If so, please describe how.

Risky Situations Online

- In the past month, have you experienced or observed any risky situations online that you did not discuss with your parent or guardian?

  – Yes
  – No

- Please describe the risky situation in a few sentences

- How did the risky situation resolve?

- Why did you choose not to discuss the risky situation with your parent or child?

- Did you use any tools during the time you observed or experienced this risky situation? If so, please describe how.

Online Risks

Please rate each of the following online risks for how likely they are, their level of severity, and how confident you are in your ability to protect yourself from them.

- How bad would it be if the you experienced the following?

Scale: Not at all bad – Extremely bad
Risks:

- Bullying another person online

- Being bullied online by another person

- Visiting sites with sexual or other adult content

- Visiting sites that urge you to use drugs or alcohol

- Visiting websites that urge you to harm yourself

- Illegally downloading copyrighted material, like music

- Getting a virus on your phone, tablet, or computer

- Texting or talking on the phone while driving

- Not getting enough sleep because of spending too much time online

- Doing poorly in school because of spending too much time online

- Having trouble with friends or family because of spending too much time online

- Being contacted by a stranger

- Being abducted by a stranger you met online

- How likely are you to experience each of the following?

Scale: Very unlikely – Very likely
Risks as above

- How confident are you that you would be able to prevent each of the following?

Scale: Not at all confident – Extremely confident
Risks as above

- How confident are you that your parent would be able to protect you from each of the following?

Scale: Not at all confident – Extremely confident
Risks as above

Parenting Strategies

Please indicate, on average, how frequently your parent or guardian does the following activities in a typical month
    Scale:

- More than once a day

- Between once a day and once a week

- Between once a week and once a month

- Less than once a month

Activities:

- Check your personal message history

- Check your social media profiles

- Take away your smartphone

- Take away your personal computer

- Remove your smartphone from your room overnight

- Discuss online safety with you

- Discuss news about online behavior with you

Software Condition

- How often did Qustodio prevent you from doing something on your smartphone?

    – More than once a day

    – Between once a day and once a week

    – Between once a week and once a month

    – Less than once a month

- Please briefly describe your experience using Qustodio. Was it helpful? Was it confusing?

- Do you feel like using Qustodio is keeping you safer online? Why or why not?

Contract Condition

- How often did your parent or guardian remind you about the terms of your contract?

    – More than once a day

    – Between once a day and once a week

    – Between once a week and once a month

    – Less than once a month

- Have you edited the terms of the contract with your parent or guardian during the past month?

    – Yes

    – No

- What did you change about the contract?

- Please briefly describe your experience using an online behavior contract. Was it helpful? Was it confusing?

- Do you feel like using an online behavior contract is keeping you safer online? Why or why not?

Control Condition

- Has your parent or guardian adopted a new parenting strategy for keeping you safe online in the past month?

    – Yes

    – No

- Please briefly describe your parent's or guardian's strategy below.

- Which of the following categories best describes your parent's or guardian's method? Check all that apply

    – Using parental controls and other software tools to monitor what you are doing online.

- Looking at your social media accounts and reading your posts and messages to monitor what you are doing online.

- Setting time limits on device use, taking away devices as punishment, or otherwise setting rules and limits on how you can use the Internet.

- Telling you about how other teenagers' unsafe online actions have had serious consequences for their personal safety to warn you against those actions.

- Teaching you about what online activity your parent/guardian consider appropriate, and how to handle potentially unsafe situations online.

- Discussing online activity and unsafe situations with you, including back-and-forth questions and sharing experiences.

- Letting you experience social media on your own, without interjecting additional information or oversight.

- Other

• Please describe your experience with this strategy. Was it helpful? Was it confusing?

• Do you feel like using this strategy is keeping you safer online? Why or why not?

Appendix D

Longitudinal Survey Study of Parenting Strategies: Materials

D.1 Entrance Survey: Parent

Demographics

The questions below ask for some basic information about you and the child with whom you will be participating in this study.

- How old are you?

- What is your sex or gender?

    – Male

    – Female

    – Other identification

    – Decline to answer

- What is your race? You may select more than one.

    – American Indian or Alaska Native

    – Asian

    – Black or African American

    – Native Hawaiian or other Pacific Islander

    – White

    – Some other race (please specify)

    – Decline to answer

- Are you Hispanic or Latino?

    – Yes

    – No

    – Decline to answer

- What is the highest level of education you have received?

- Less than high school degree
- High school degree or equivalent (e.g., GED)
- Some college but no degree
- Associate degree
- Bachelor degree
- Graduate degree
- Decline to answer

- What is your household income?

  - Less than $20,000
  - $20,000 to $34,999
  - $35,000 to $49,999
  - $50,000 to $74,999
  - $75,000 to $99,999
  - $100,000 to $149,999
  - $150,000 to $199,999
  - $200,000 or more
  - Decline to answer

- What is your marital status? Please check all that apply.

  - Widowed
  - Divorced
  - Separated
  - Living with partner
  - Married
  - Never married
  - Decline to answer

- What is the birthdate of your child who will also be taking part in this study?

- What is the gender of your child who will also be taking part in this study?

  - Male
  - Female
  - Other
  - Decline to answer

- What type of school does your child attend?

  - Public
  - Private
  - Charter

- Home school
- Other

• How many students are enrolled at your child's school?

- 500 or fewer
- 501 - 1000
- 1001 - 1500
- 1501 - 2000
- 2001 - 2500
- 2501 - 3000
- More than 3000 students

• What is the grade range of your child's school? For example, a typical four-year high school would be grades 9 - 12, and a school that combines kindergarten through eighth grade students would be K - 8.

- K - 4
- K - 5
- K - 6
- K - 8
- K - 12
- 5 - 8
- 6 - 8
- 7 - 9
- 6 - 12
- 9 - 12
- 10 - 12
- Other

• In the past year, has your child's school ever contacted you about your child getting in trouble for their behavior?

- Yes
- No
- I don't know

• How many times has your child's school contacted you in the past year about your child getting in trouble for their behavior?

On the following pages you will be asked questions about social media, which includes platforms such as Facebook, Instagram, Twitter, Snapchat, Tumblr and other places where people interact online.

You will also periodically be asked questions that refer to "your child," which here indicates the child with whom you are participating in this study.

• Why did you choose to get your child a smartphone?

• What online safety risks to your child worry you?

157

Screen Time

On an average day, how many hours does your child use their smartphone?* If you do not wish to enter a range, you may enter the same value for both minimum and maximum hours.

- Minimum hours per day

- Maximum hours per day

How often does your child use their phone during the following times?
Scale:

- Never

- Rarely

- Sometimes

- Often

- This does not apply to my child

Times:

- During a meal

- After they go to bed

- Before breakfast in the morning

- During school

- During after-school activities

- During a free period in school

- When your child is hanging out with friends

- When your child is a passenger in a car

- When your child is a passenger on a bus or public transportation

- While your child is waiting in line

- When your child is talking to you

Cyberbullying and Drama Scenarios

(The following scenarios were shown in a random order to participants. Characters in the scenarios were matched to the child's gender.)

$e://Field/name, a high school student, sees a post about$e://Field/selfon social media made by a friend. The post is making fun of$e://Field/name, and$e://Field/subjectwishes the friend would not have made the post, so$e://Field/subjectresponds defensively. The friend then replied, "Can't you take a joke?" Both$e://Field/nameand$e://Field/possessivefriend have a few likes on their comments, and people at school talk about the exchange for a few weeks after.

- Which of the following statements describe this situation? (Check as many as apply.)

    - My child has done this kind of thing in the past (like what $e://Field/name did)
    - This kind of thing has happened to my child in the past (My child has been on the receiving end of the kind of thing that $e://Field/name did)
    - This kind of behavior is common
    - This kind of behavior is appropriate
    - This is bullying
    - This is typical teen drama
    - This sounds like a fun interaction
    - This reflects poor judgment
    - This kind of behavior is annoying to others
    - Other (please describe)

$e://Field/name2, a high school student, sees a post about$e://Field/selfon social media made by a classmate. The post is making fun of$e://Field/name2, and has a lot of likes and comments from other classmates adding on.$e://Field/name2's classmate has made a similar post about$e://Field/name2almost every day this week, and$e://Field/name2feels hurt by these posts.

- Which of the following statements describe this situation? (Check as many as apply.)

    - My child has done this kind of thing in the past (like what $e://Field/name2 did)
    - This kind of thing has happened to my child in the past (My child has been on the receiving end of the kind of thing that $e://Field/name2 did)
    - This kind of behavior is common
    - This kind of behavior is appropriate
    - This is bullying
    - This is typical teen drama
    - This sounds like a fun interaction
    - This reflects poor judgment
    - This kind of behavior is annoying to others
    - Other (please describe)

- What does cyberbullying mean to you?

- What does typical online drama mean to you?

Online Risks

Over the next few pages, you will be asked to rate a set of situations for their level of severity, how likely they are, how confident you are in your own ability and your child's ability to prevent them from happening.
Question:

- How bad are each of the following situations?

159

Scale: Not at all bad – Extremely bad
Risks:

- My child bullies another person online

- My child is bullied online by another person

- My child comes across sites with sexual or other adult content

- My child seeks out sites with sexual or other adult content

- My child comes across online content that encourages the use of drugs or alcohol

- My child seeks out online content that encourages the use of drugs or alcohol

- My child comes across websites that urge them to harm themself

- My child seeks out websites that urge them to harm themself

- My child illegally downloads copyrighted material, like music

- My child gets a virus on their phone, tablet, or computer

- My child texts on their phone while driving

- My child spends too much time using their phone, laptop, or other digital device

- My child does not get enough sleep because of spending too much time online

- My child does poorly in school because of spending too much time online

- My child has trouble with friends or family because of spending too much time online

- My child is contacted by a stranger online

- My child is kidnapped by a stranger they met online

- My child is shown an online advertisement

Question:

- How likely is your child to experience or do the following?

Scale: Very unlikely – Very likely
Risks as above
Question:

- How confident are you that your child would avoid or be able to prevent each of the following?

Scale: Not at all confident – Extremely confident
Risks as above

- How confident are you that you would be able to protect your child from or prevent each of the following?

Scale: Not at all confident – Extremely confident
Risks as above

Parenting Strategies

Please indicate how frequently you use each of the following parenting strategies.

- Using parental controls and other software tools to monitor what your child is doing online.

  - This is a primary strategy for me
  - This is a secondary strategy for me
  - I occasionally use this strategy
  - I do not use this strategy

- Please briefly describe how you use this strategy.

- Looking at your child's social media accounts and reading their posts and messages to monitor what they are doing online.

  - This is a primary strategy for me
  - This is a secondary strategy for me
  - I occasionally use this strategy
  - I do not use this strategy

- Please briefly describe how you use this strategy.

- Setting time limits on device use, taking away devices as punishment, or otherwise setting rules and limits on how your child can use the Internet.

  - This is a primary strategy for me
  - This is a secondary strategy for me
  - I occasionally use this strategy
  - I do not use this strategy

- Please briefly describe how you use this strategy.

- Telling your child about how other teenagers' unsafe online actions have had serious consequences for their personal safety to warn against those actions.

  - This is a primary strategy for me
  - This is a secondary strategy for me
  - I occasionally use this strategy
  - I do not use this strategy

- Please briefly describe how you use this strategy.

- Teaching your child about what online activity you consider appropriate, and how to handle potentially unsafe situations online.

  - This is a primary strategy for me
  - This is a secondary strategy for me
  - I occasionally use this strategy

– I do not use this strategy

- Please briefly describe how you use this strategy.

- Discussing online activity and unsafe situations with your child, including back-and-forth questions and sharing experiences.

    – This is a primary strategy for me
    – This is a secondary strategy for me
    – I occasionally use this strategy
    – I do not use this strategy

- Please briefly describe how you use this strategy.

- Letting your child experience social media on their own, without interjecting additional information or oversight.

    – This is a primary strategy for me
    – This is a secondary strategy for me
    – I occasionally use this strategy
    – I do not use this strategy

- Please briefly describe how you use this strategy.

- Are there any other adults in your household or in your child's life who employ parenting strategies to keep your child safe online?

    – Yes
    – No

- Briefly describe who these adults are and what strategies they are using to keep your child safe online.

Please indicate, on average, how frequently you do the following activities in a typical month. Scale:

- Once a day or more

- About once or twice a week

- About once or twice a month

- Less than once a month

- Never

- This does not apply to my child

Activities:

- Check your child's personal message history

- Check your child's social media profiles

- Take away your child's smartphone

- Take away your child's personal computer

- Remove your child's smartphone from their room overnight

- Discuss online safety with your child

- Discuss news about online behavior with your child

D.2   Entrance Survey: Child

Demographics

The questions below ask for some basic information about you.

- What is your birthdate?

- What is your sex or gender?

  – Male
  – Female
  – Other identification
  – Decline to answer

- What is your race? You may select more than one.

  – American Indian or Alaska Native
  – Asian
  – Black or African American
  – Native Hawaiian or other Pacific Islander
  – White
  – Some other race (please specify)
  – Decline to answer

- Are you Hispanic or Latino?

  – Yes
  – No
  – Decline to answer

- What grades do you typically receive in school?

  – Mostly As and Bs
  – Mostly Bs and Cs
  – Mostly Cs and Ds
  – Mostly Ds and below

– Decline to answer

- What is your email address?

On the following pages you will be asked questions about social media, which includes platforms such as Facebook, Instagram, Twitter, Snapchat, Tumblr and other places where people interact online.

You should understand that if your responses to this survey indicate you or someone else is at risk of serious harm, we will take the necessary action to report this to authorities, such as law enforcement. This may include reporting your personal information, including name or address. For example, we will report any cases of child abuse.

- Why did you want to get a smartphone?

- What unsafe things online worry you?

Screen Time

- On an average day, how many hours do you use your smartphone? If you do not wish to enter a range, you may enter the same value for both minimum and maximum hours.

  – Minimum hours per day
  – Maximum hours per day

How often do you use your phone during the following times?
Scale:

- Never

- Rarely

- Sometimes

- Often

- This does not apply to me

Times:

- During a meal

- After you go to bed

- Before breakfast in the morning

- During school

- During after-school activities

- During a free period in school

- When you are hanging out with friends

- When you are a passenger in a car

- When you are a passenger on a bus or public transportation

- While you are waiting in line

- When you are talking to your parents

Cyberbullying and Drama Scenarios

(The following scenarios were shown in a random order to participants. Characters in the scenarios were matched to the child's gender.)

$e://Field/name, a high school student, sees a post about$e://Field/selfon social media made by a friend. The post is making fun of$e://Field/name, and$e://Field/subjectwishes the friend would not have made the post, so$e://Field/subjectresponds defensively. The friend then replied, "Can't you take a joke?" Both$e://Field/nameand$e://Field/possessivefriend have a few likes on their comments, and people at school talk about the exchange for a few weeks after.

- Which of the following statements describe this situation? (Check as many as apply.)

  - I have done this kind of thing in the past (like what $e://Field/name did)
  - This kind of thing has happened to me in the past (I have been on the receiving end of the kind of thing that $e://Field/name did)
  - This kind of behavior is common
  - This kind of behavior is appropriate
  - This is bullying
  - This is typical teen drama
  - This sounds like a fun interaction
  - This reflects poor judgment
  - This kind of behavior is annoying to others
  - Other (please describe)

$e://Field/name2, a high school student, sees a post about$e://Field/selfon social media made by a classmate. The post is making fun of$e://Field/name2, and has a lot of likes and comments from other classmates adding on.$e://Field/name2's classmate has made a similar post about$e://Field/name2almost every day this week, and$e://Field/name2feels hurt by these posts.

- Which of the following statements describe this situation? (Check as many as apply.)

  - I have done this kind of thing in the past (like what $e://Field/name2 did)
  - This kind of thing has happened to me in the past (I have been on the receiving end of the kind of thing that $e://Field/name2 did)
  - This kind of behavior is common
  - This kind of behavior is appropriate
  - This is bullying
  - This is typical teen drama
  - This sounds like a fun interaction
  - This reflects poor judgment

165

      – This kind of behavior is annoying to others

      – Other (please describe)

- What does cyberbullying mean to you?

- What does typical online drama mean to you?

Online Risks

Over the next few pages, you will be asked to rate a set of situations for their level of severity, how likely they are, how confident you are in your parent's ability and your own ability to prevent them from happening.

Question:

- How bad are each of the following situations?

Scale: Not at all bad – Extremely bad

- I bully another person online

- I am bullied online by another person

- I come across sites with sexual or other adult content

- I seek out sites with sexual or other adult content

- I come across online content that encourages the use of drugs or alcohol

- I seek out online content that encourages the use of drugs or alcohol

- I come across websites that urge me to harm myself

- I seek out websites that urge me to harm myself

- I illegally download copyrighted material, like music

- I get a virus on my phone, tablet, or computer

- I text on my phone while driving

- I spend too much time using my phone, laptop, or other digital device

- I do not get enough sleep because of spending too much time online

- I do poorly in school because of spending too much time online

- I have trouble with friends or family because of spending too much time online

- I am contacted by a stranger online

- I am kidnapped by a stranger I met online

- I am shown an online advertisement

Question:

- How likely are you to experience or do the following?

Scale: Very unlikely – Very likely
Risks as above
Question:

- How confident are you that you would avoid or be able to prevent each of the following?

Scale: Not at all confident – Extremely confident
Risks as above
Question:

- How confident are you that your parent would be able to protect you from or prevent each of the following?

Scale: Not at all confident – Extremely confident
Risks as above

Parenting Strategies

- Briefly describe something your parent or guardian is currently doing to protect you from online risks.

- Which of the following categories best describes your parent's or guardian's method that you described above? Check all that apply.

   – Using parental controls and other software tools to monitor what you are doing online.
   – Looking at your social media accounts and reading your posts and messages to monitor what you are doing online.
   – Setting time limits on device use, taking away devices as punishment, or otherwise setting rules and limits on how you can use the Internet.
   – Telling you about how other teenagers' unsafe online actions have had serious consequences for their personal safety to warn you against those actions.
   – Teaching you about what online activity your parent/guardian consider appropriate, and how to handle potentially unsafe situations online.
   – Discussing online activity and unsafe situations with you, including back-and-forth questions and sharing experiences.
   – Letting you experience social media on your own, without interjecting additional information or oversight.
   – Other

Please indicate, on average, how frequently your parent or guardian does the following activities in a typical month
Scale:

- Once a day or more

- About once or twice a week

- About once or twice a month

- Less than once a month

- Never

- This does not apply to me

Activities:

- Check your personal message history

- Check your social media profiles

- Take away your smartphone

- Take away your personal computer

- Remove your smartphone from your room overnight

- Discuss online safety with you

- Discuss news about online behavior with you

D.3   Condition Assignment Survey

For the next part of this study, please follow the directions below. Note that you must complete everything described on the following page to finish the entrance requirements of this study and receive your compensation.   If you have any questions about these instructions, please email teeninternetstudy@cups.cs.cmu.edu for assistance. If you need to complete these tasks at a later time, you can always return to this survey.

Software Condition

Your task is to install the parenting software Qustodio on the smartphone belonging to the child with whom you are participating in this study. As part of this study, we are providing you with a free license to use this software, and in exchange, you must use the password we provide to register your account.   Open the following URL in a new browser tab or window: www.qustodio.com/signup The sign up page will first prompt you for a license code for Qustodio. Enter the following license code: $e://Field/license When you move to the next step, you will be prompted to register an account with Qustodio. Register an account as you normally would, using your (the parent's) email address, but when prompted for a password, use the following: $e://Field/password You MUST register your account with this password to continue with this study. Note that this account will control what the Qustodio software does, and if you would not like your child to have access to the Qustodio control panel, you should not share this password with them.   As part of the registration process, Qustodio will ask you for an email address to provide a download link for their software. You should provide an email address that your child can access on their smartphone (e.g., your child's email address), as Qustodio will use this email to send a download link and installation instructions to that device. If your child does not have an email address of their own, you can download the Qustodio app from the Google Play Store or Apple App Store directly.   Once you have completed your account registration, you must set up Qustodio to begin monitoring your

child's device. This can be done either alone or with your child. To set up Qustodio on your child's device, you must install the Qustodio app on their smartphone. When the app has finished installing, open the app, and enter the username and password for the account you registered on the Qustodio website. Once logged in, the Qustodio app will walk you through a set up and installation process. Follow the provided instructions until the app confirms that set up is complete. Once your child's device has been set up to use Qustodio, return to a computer to set what Qustodio will monitor. Return to the Qustodio website if you closed it (https://www.qustodio.com/en/) and make sure you are logged in. You should be shown an "Activity Summary" page for your child's smartphone. Look for a grey tab labeled "Rules," with a gear icon, in the row of blue tabs that offer details of your child's smartphone activity. Click the "Rules" tab. You should now be on a page which allows you to configure the types of content that are and are not allowed to be accessed by your child's smartphone. Additionally, there is a grey header menu which links to this page and six other pages which allow you to specify other rules for the Qustodio software. Visit each of these rules pages in turn, and look at all of the settings you have available. Modify them in whatever way you would likeconfigure Qustodio as you would actually like a parenting software to function. Make sure to visit all seven of these rules pages. Once you have registered your Qustodio account, installed Qustodio on your child's smartphone, and configured the settings you would like for Qustodio, you have almost finished the first part of the study!

If you have any questions about these instructions, please emailteeninternetstudy@cups.cs.cmu.edufor assistance.

- Please describe, in a few sentences, your experience of setting up Qustodio.

- How long did it take to set up Qustodio, in minutes?

- Did you have to turn off WiFi to install Qustodio on your child's phone?

  – Yes

  – No

- How easy or difficult was setting up this software with your child?

  – Scale: Extremely easy – Extremely difficult

- What was the most interesting part of setting up Qustodio?

- What was the most difficult part of setting up Qustodio?

- What was the most useful part of setting up Qustodio?

Contract Condtion

Your task is to create a contract between you and the child with whom you are participating in this study. The contract will give you a set of rules about your child's online behavior that both you and your child agree on. For this task, you will be using the contract tool provided by The Smart Talk, which is available at the following URL (Please open this in a new browser tab or window, and we strongly suggest that this task be completed on a desktop or laptop computer): https://thesmarttalk.org/ Note that to create this contract, you do not need to provide any personal information or register an account. The contract will prompt you for your name and your child's name, which will be used to personalize the contract for you. If you would not like to provide your names, feel free to use a nickname. To create this contract, find a time when you

169

and your child are both available for roughly half an hour. Once you are both ready, navigate to the The Smart Talk website, and click the red "Get Me Started" button to begin. You will first be prompted for your names (as mentioned above), and once those are provided, you will be prompted with questions about how you would like to set up your online behavior expectations for your child. Follow the prompts on screen until you have completed the contract. Once you have completed the contract, you are offered the opportunity to print the final document. Please click the button to print, and save the document as a PDF file. The following links provide instructions for how to print a document to a PDF file for both Windows and Mac operating systems. Again, please open these in a new browser tab or window. Windows: https://www.howtogeek.com/150891/how-to-print-to-pdf-in-windows-4-tips-and-tricks/ Mac: http://osxdaily.com/2010/05/21/how-to-print-to-pdf-in-mac-os/ If you cannot save this file to a PDF, please take photos of your contract and save them to your computer, or print the contract to a physical printer, and then scan the printed contract so that it is saved as a digital file. Make sure you have saved a copy of this contract in a safe place on your computer! If you have any questions about these instructions, please emailteeninternetstudy@cups.cs.cmu.edufor assistance.

- Upload the contract that you and your child created.

- Please describe, in a few sentences, your experience of setting up the contract.

- How long did it take to set up the contract, in minutes?

- How easy or difficult was setting up this contract with your child?

    - Scale: Extremely easy – Extremely difficult

- What was the most interesting part of setting up this contract?

- What was the most difficult part of setting up this contract?

- What was the most useful part of setting up this contract?

Control Condition

Your task is to have a conversation with your child about your household rules and expectations around your child's online behavior. To complete this task, find a time when you and your child are both available for roughly half an hour. Once you are both ready, you should begin to discuss your responses to the following question: "What are your household rules and expectations about how your child uses the internet and digital devices (e.g. smartphone, computers)?"

You may conduct the conversation about household rules however you see fit. If you have any questions about these instructions, please emailteeninternetstudy@cups.cs.cmu.edufor assistance.

- Please describe, in a few sentences, what you and your child discussed.

- How long did this conversation take, in minutes?

- How easy or difficult was having this conversation with your child?

    - Scale: Extremely easy – Extremely difficult

- What was the most interesting part of this conversation?

- What was the most difficult part of this conversation?

- What was the most useful part of this conversation?

D.4 Exit Survey: Parent

On the following pages you will be asked questions about social media, which includes platforms such as Facebook, Instagram, Twitter, Snapchat, Tumblr and other places where people interact online.

- What online safety risks to your child worry you?

Discussions or Disagreement About Online Safety

- Have you and your child had any discussions or disagreements about online activity in the past month?For example, have you talked about a news story that mentioned social media? Have you punished your child for something done online? Have you talked about something your child is doing online?

    – Yes

    – No

- Please describe your interaction in a few sentences

- In your opinion, what caused the interaction?

- How did the interaction resolve?

- Did you use any tools during the course of this interaction? If so, please describe how.

Risky Situations Online

- In the past month, have you observed your child experiencing any risky situations online, which you did not discuss with your child?

    – Yes

    – No

- Please describe the risky situation in a few sentences

- How did the risky situation resolve?

- Why did you choose not to discuss the risky situation with your child?

- Did you use any tools during the time you observed this risky situation? If so, please describe how.

Screen Time

On an average day, how many hours does your child use their smartphone?* If you do not wish to enter a range, you may enter the same value for both minimum and maximum hours.

- Minimum hours per day

- Maximum hours per day

How often does your child use their phone during the following times?
Scale:

- Never

- Rarely

- Sometimes

- Often

- This does not apply to my child

Times:

- During a meal

- After they go to bed

- Before breakfast in the morning

- During school

- During after-school activities

- During a free period in school

- When your child is hanging out with friends

- When your child is a passenger in a car

- When your child is a passenger on a bus or public transportation

- While your child is waiting in line

- When your child is talking to you

Online Risks

Over the next few pages, you will be asked to rate a set of situations for their level of severity, how likely they are, how confident you are in your own ability and your child's ability to prevent them from happening.
Question:

- How bad are each of the following situations?

Scale: Not at all bad – Extremely bad
Risks:

- My child bullies another person online

- My child is bullied online by another person

- My child comes across sites with sexual or other adult content

- My child seeks out sites with sexual or other adult content

- My child comes across online content that encourages the use of drugs or alcohol

- My child seeks out online content that encourages the use of drugs or alcohol

- My child comes across websites that urge them to harm themself

- My child seeks out websites that urge them to harm themself

- My child illegally downloads copyrighted material, like music

- My child gets a virus on their phone, tablet, or computer

- My child texts on their phone while driving

- My child spends too much time using their phone, laptop, or other digital device

- My child does not get enough sleep because of spending too much time online

- My child does poorly in school because of spending too much time online

- My child has trouble with friends or family because of spending too much time online

- My child is contacted by a stranger online

- My child is kidnapped by a stranger they met online

- My child is shown an online advertisement

Question:

- How likely is your child to experience or do the following?

Scale: Very unlikely – Very likely
Risks as above
Question:

- How confident are you that your child would avoid or be able to prevent each of the following?

Scale: Not at all confident – Extremely confident
Risks as above

- How confident are you that you would be able to protect your child from or prevent each of the following?

Scale: Not at all confident – Extremely confident
Risks as above

Parenting Strategies

Please indicate, on average, how frequently you do the following activities in a typical month.
Scale:

- Once a day or more

- About once or twice a week

- About once or twice a month

- Less than once a month

- Never

- This does not apply to my child

Activities:

- Check your child's personal message history

- Check your child's social media profiles

- Take away your child's smartphone

- Take away your child's personal computer

- Remove your child's smartphone from their room overnight

- Discuss online safety with your child

- Discuss news about online behavior with your child

Software Condition

- How often did you log in to the parent control panel for Qustodio?

  - More than once a day
  - Between once a day and once a week
  - Between once a week and once a month
  - Less than once a month

- How often did you get an alert from Qustodio about your child's online activity?

  - More than once a day
  - Between once a day and once a week
  - Between once a week and once a month
  - Less than once a month

- Did you edit the settings for Qustodio during the past month?

  - Yes
  - No

- What settings have you changed?

- Please briefly describe your experience using Qustodio. Was it helpful? Was it confusing?

- Do you feel like using Qustodio is keeping your child safer online? Why or why not?

Contract Condition

- How often did you review the contract you had written?

  - More than once a day
  - Between once a day and once a week
  - Between once a week and once a month
  - Less than once a month

- How often did you remind your child about the terms of your contract?

  - More than once a day
  - Between once a day and once a week
  - Between once a week and once a month
  - Less than once a month

- Have you edited the terms of the contract during the past month?

  - Yes
  - No

- What did you change about the contract?

- Please briefly describe your experience using an online behavior contract. Was it helpful? Was it confusing?

- Do you feel like using an online behavior contract is keeping your child safer online? Why or why not?

Control Condition

- Have you adopted a new parenting strategy for keeping your child safe online in the past month?

  - Yes
  - No

- Please briefly describe your parenting strategy below.

- Which of the following categories best describes your strategy? Check all that apply.

  - Using parental controls and other software tools to monitor what your child is doing online.
  - Looking at you child's social media accounts and reading their posts and messages to monitor what your child is doing online.

- Setting time limits on device use, taking away devices as punishment, or otherwise setting rules and limits on how your child can use the Internet.

- Telling your child about how other teenagers' unsafe online actions have had serious consequences for their personal safety to warn against those actions.

- Teaching your child about what online activity you consider appropriate, and how to handle potentially unsafe situations online.

- Discussing online activity and unsafe situations with your child, including back-and-forth questions and sharing experiences.

- Letting your child experience social media on their own, without interjecting additional information or oversight.

- Other

• Please describe your experience using this strategy. Was it helpful? Was it confusing?

• Do you feel like using this strategy is keeping your child safer online? Why or why not?

D.5 Exit Survey: Child

On the following pages you will be asked questions about social media, which includes platforms such as Facebook, Instagram, Twitter, Snapchat, Tumblr and other places where people interact online.

• What unsafe things online worry you?

Discussions or Disagreement About Online Safety

• Have you and your parent or guardian had any discussions or disagreements about online activity in the past month? For example, have you talked about a news story that mentioned social media? Have you received a punishment for something done online? Have you talked about something you are doing online?

- Yes
- No

• Please describe your interaction in a few sentences

• In your opinion, what caused the interaction?

• How did the interaction resolve?

• Did you use any tools during the course of this interaction? If so, please describe how.

Risky Situations Online

• In the past month, have you experienced or observed any risky situations online that you did not discuss with your parent or guardian?

- Yes
- No

- Please describe the risky situation in a few sentences

- How did the risky situation resolve?

- Why did you choose not to discuss the risky situation with your parent or guardian?

- Did you use any tools during the time you observed or experienced this risky situation? If so, please describe how.

Screen Time

- On an average day, how many hours do you use your smartphone? If you do not wish to enter a range, you may enter the same value for both minimum and maximum hours.

    – Minimum hours per day
    – Maximum hours per day

How often do you use your phone during the following times?
Scale:

- Never

- Rarely

- Sometimes

- Often

- This does not apply to me

Times:

- During a meal

- After you go to bed

- Before breakfast in the morning

- During school

- During after-school activities

- During a free period in school

- When you are hanging out with friends

- When you are a passenger in a car

- When you are a passenger on a bus or public transportation

- While you are waiting in line

- When you are talking to your parents

Online Risks

Over the next few pages, you will be asked to rate a set of situations for their level of severity, how likely they are, how confident you are in your parent's ability and your own ability to prevent them from happening.

Question:

• How bad are each of the following situations?

Scale: Not at all bad – Extremely bad

• I bully another person online

• I am bullied online by another person

• I come across sites with sexual or other adult content

• I seek out sites with sexual or other adult content

• I come across online content that encourages the use of drugs or alcohol

• I seek out online content that encourages the use of drugs or alcohol

• I come across websites that urge me to harm myself

• I seek out websites that urge me to harm myself

• I illegally download copyrighted material, like music

• I get a virus on my phone, tablet, or computer

• I text on my phone while driving

• I spend too much time using my phone, laptop, or other digital device

• I do not get enough sleep because of spending too much time online

• I do poorly in school because of spending too much time online

• I have trouble with friends or family because of spending too much time online

• I am contacted by a stranger online

• I am kidnapped by a stranger I met online

• I am shown an online advertisement

Question:

• How likely are you to experience or do the following?

Scale: Very unlikely – Very likely
Risks as above
Question:

• How confident are you that you would avoid or be able to prevent each of the following?

Scale: Not at all confident – Extremely confident
Risks as above
Question:

- How confident are you that your parent would be able to protect you from or prevent each of the following?

Scale: Not at all confident – Extremely confident
Risks as above

Parenting Strategies

Please indicate, on average, how frequently your parent or guardian does the following activities in a typical month
Scale:

- Once a day or more

- About once or twice a week

- About once or twice a month

- Less than once a month

- Never

- This does not apply to me

Activities:

- Check your personal message history

- Check your social media profiles

- Take away your smartphone

- Take away your personal computer

- Remove your smartphone from your room overnight

- Discuss online safety with you

- Discuss news about online behavior with you

Software Condition

- How often did Qustodio prevent you from doing something on your smartphone?

  - More than once a day
  - Between once a day and once a week
  - Between once a week and once a month
  - Less than once a month

- Please briefly describe your experience using Qustodio. Was it helpful? Was it confusing?

- Do you feel like using Qustodio is keeping you safer online? Why or why not?

Contract Condition

- How often did your parent or guardian remind you about the terms of your contract?

  – More than once a day
  – Between once a day and once a week
  – Between once a week and once a month
  – Less than once a month

- Have you edited the terms of the contract with your parent or guardian during the past month?

  – Yes
  – No

- What did you change about the contract?

- Please briefly describe your experience using an online behavior contract. Was it helpful? Was it confusing?

- Do you feel like using an online behavior contract is keeping you safer online? Why or why not?

Control Condition

- Has your parent or guardian adopted a new parenting strategy for keeping you safe online in the past month?

  – Yes
  – No

- Please briefly describe your parent's or guardian's strategy below.

- Which of the following categories best describes your parent's or guardian's method? Check all that apply

  – Using parental controls and other software tools to monitor what you are doing online.
  – Looking at your social media accounts and reading your posts and messages to monitor what you are doing online.
  – Setting time limits on device use, taking away devices as punishment, or otherwise setting rules and limits on how you can use the Internet.
  – Telling you about how other teenagers' unsafe online actions have had serious consequences for their personal safety to warn you against those actions.
  – Teaching you about what online activity your parent/guardian consider appropriate, and how to handle potentially unsafe situations online.
  – Discussing online activity and unsafe situations with you, including back-and-forth questions and sharing experiences.
  – Letting you experience social media on your own, without interjecting additional information or oversight.

– Other

- Please describe your experience with this strategy. Was it helpful? Was it confusing?

- Do you feel like using this strategy is keeping you safer online? Why or why not?

Appendix E

Cyberbullying and Drama: Supplementary Tables

E.1 Bullying and Drama Scenario Response Model

E.1.1 Interviews

Results of a generalized binomial mixed model fit by maximum likelihood

AIC	BIC	logLik	deviance	df.resid
151.0	184.8	-63.5	127.0	112

Scaled residuals:

Min	1Q	Median	3Q	Max
-4.2985	-0.8908	0.2246	0.6924	1.2510

Random effects:

Groups	Name	Variance	Std.Dev.
id	(Intercept)	0	0

Number of obs: 124, groups: id, 31

Fixed Effect	Estimate	p
(Intercept)	3.0591	0.00776 **
participant	-0.1425	0.89952
scenario (drama)	-1.7490	0.17186
label (drama)	-3.2291	0.00736 **
scenario gender (male)	15.4958	0.97169
label (drama) by scenario gender (male)	-14.1641	0.97412
scenario (drama) by scenario gender (male)	-16.2049	0.97039
scenario (drama) by label (drama)	2.7011	0.05064 .
participant by scenario (drama)	-0.3335	0.73116
participant by label (drama)	-0.1354	0.89170
scenario (drama) by label (drama) by scenario gender (male)	14.4712	0.97356
Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1		

Table E.1: Model of interview participants' responses to bullying and drama scenarios, which examines primarily interactions between the factors of scenario, the label applied to the scenario by the participant, participant age, and gender of the character in the scenario.

184

E.1.2 Surveys

Results of a generalized binomial mixed model fit by maximum likelihood

AIC	BIC	logLik	deviance	df.resid
763.6	826.9	-367.8	735.6	666

Scaled residuals:

Min	1Q	Median	3Q	Max
-3.9047	-0.6788	0.2422	0.7544	2.4049

Random effects:

Groups	Name	Variance	Std.Dev.
id	(Intercept)	0.31	0.5568
first scenario	(Intercept)	0.00	0.0000

Number of obs: 680, groups: id, 92; first scenario, 2

Fixed Effect	Estimate	p
(Intercept)	2.39424	5.55e-07 ***
participant (parent)	0.49491	0.38564
scenario (drama)	-1.67062	0.00234 **
label (drama)	-3.00417	7.36e-08 ***
scenario gender (male)	-0.22480	0.69784
label (drama) by scenario gender (male)	-0.16483	0.80818
scenario (drama) by scenario gender (male)	-0.10712	0.87012
scenario (drama) by label (drama)	2.46676	0.00030 ***
participant (parent) by scenario (drama)	-0.55734	0.39723
participant (parent) by label (drama)	-1.20785	0.07500 .
scenario (drama) by label (drama) by scenario gender (male)	-0.01352	0.98685
participant (parent) by scenario (drama) by label (drama)	0.95650	0.24351

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Table E.2: Model of survey participants' responses to bullying and drama scenarios, which examines primarily interactions between the factors of scenario, the label applied to the scenario by the participant, participant age, and gender of the character in the scenario.

E.2 Bullying and Drama Code Use Model

Results of a generalized binomial mixed model fit by maximum likelihood

AIC	BIC	logLik	deviance	df.resid
2800.0	3495.4	-1294.0	2588.0	5114

Scaled residuals:

Min	1Q	Median	3Q	Max
-5.2248	-0.3365	-0.1686	0.0000	10.1117

Random effects:

Groups	Name	Variance	Std.Dev.
Family	(Intercept)	0.1539	0.3923

Number of obs: 5220, groups: Family, 94

Fixed Effect	Estimate	p
Intercept	-2.733e-01	0.43768
participant (parent)	-1.273e-01	0.78156
code (anger)	-1.969e+01	0.99539
code (back and forth)	-1.929e+01	0.99505
code (communication control)	-2.293e-01	0.64701
code (conditional reaction)	-1.690e+00	0.00855 **
code (nonreaction)	-8.173e-01	0.12954
code (exaggeration)	-2.031e+01	0.99618
code (hurt reaction)	2.102e-01	0.67114
code (intent to hurt)	2.926e+00	.01e-05 ***
code (permanence)	-2.464e+00	0.00258 **
code (permission)	-1.198e+00	0.03708 *
code (power imbalance)	-6.171e-01	0.23003
code (repetition)	1.251e+00	0.01535 *
code (serious harm)	-2.275e+00	0.00236 **
scenario (drama)	-5.179e-01	0.27172
study type (survey)	-2.122e+00	.72e-05 ***
code (anger) by study type (survey)	9.451e-01	0.99982
code (back and forth) by study type (survey)	1.841e+01	0.99527
code (communication control) by study type (survey)	5.811e-01	0.43384
code (conditional reaction) by study type (survey)	-3.256e+01	0.99264
code (nonreaction) by study type (survey)	-1.728e+01	0.99483
code (exaggeration) by study type (survey)	2.171e+00	0.99962
code (hurt reaction) by study type (survey)	-1.102e+00	0.21813
code (intent to hurt) by study type (survey)	-3.426e-01	0.67516
code (permanence) by study type (survey)	-1.570e+01	0.99632
code (permission) by study type (survey)	-3.966e-01	0.74882
code (power imbalance) by study type (survey)	9.064e-02	0.91168
code (repetition) by study type (survey)	-6.488e-01	0.36913
code (serious harm) by study type (survey)	2.027e+00	0.03903 *
scenario (drama) by study type (survey)	1.269e+00	0.02178 *
participant (parent) by study type (survey)	1.200e+00	0.03106 *
participant (parent) by code (anger)	1.662e+01	0.99611
participant (parent) by code (back and forth)	-3.375e+01	0.99346
participant (parent) by code (communication control)	-6.053e-01	0.38954
participant (parent) by code (conditional reaction)	8.189e-01	0.32522
participant (parent) by code (nonreaction)	1.273e-01	0.86418
participant (parent) by code (exaggeration)	1.655e-01	0.99997

participant (parent) by code (hurt reaction)	-4.316e-01	0.52562
participant (parent) by code (intent to hurt)	3.013e-01	0.70920
participant (parent) by code (permanence)	1.273e-01	0.91141
participant (parent) by code (permission)	-3.645e-01	0.66652
participant (parent) by code (power imbalance)	7.889e-01	0.24487
participant (parent) by code (repetition)	3.592e-01	0.60566
participant (parent) by code (serious harm)	8.825e-01	0.34495
code (anger) by scenario (drama)	1.925e+01	0.99549
code (back and forth) by scenario (drama)	1.737e+01	0.99554
code (communication control) by scenario (drama)	-8.507e-01	0.26287
code (conditional reaction) by scenario (drama)	-2.230e-01	0.82896
code (nonreaction) by scenario (drama)	1.772e-01	0.81994
code (exaggeration) by scenario (drama)	1.884e+01	0.99645
code (hurt reaction) by scenario (drama)	-1.353e+00	0.07914 .
code (intent to hurt) by scenario (drama)	-1.835e+00	0.02232 *
code (permanence) by scenario (drama)	-1.822e-01	0.89298
code (permission) by scenario (drama)	-2.681e-01	0.76617
code (power imbalance) by scenario (drama)	-5.807e-01	0.44704
code (repetition) by scenario (drama)	-1.964e+00	0.00630 **
code (serious harm) by scenario (drama)	-8.648e-01	0.52053
participant (parent) by scenario (drama)	-6.273e-01	0.25866
participant (parent) by code (anger) by study type (survey)	-1.676e+01	0.99655
participant (parent) by code (back and forth) by study type (survey)	1.603e+01	0.99595
participant (parent) by code (communication control) by study type (survey)	-2.000e+00	0.04055 *
participant (parent) by code (conditional reaction) by study type (survey)	1.501e+01	0.99533
participant (parent) by code (nonreaction) by study type (survey)	-1.298e+00	0.41165
participant (parent) by code (exaggeration) by study type (survey)	-1.252e+00	0.29508
participant (parent) by code (hurt reaction) by study type (survey)	-8.121e-01	0.43879
participant (parent) by code (intent to hurt) by study type (survey)	-2.019e-01	0.80884
participant (parent) by code (permanence) by study type (survey)	-1.181e+00	0.99975
participant (parent) by code (permission) by study type (survey)	5.428e-01	0.71126
participant (parent) by code (power imbalance) by study type (survey)	-4.970e-01	0.57814
participant (parent) by code (repetition) by study type (survey)	-9.748e-01	0.24016
participant (parent) by code (serious harm) by study type (survey)	-1.727e+00	0.13916
code (anger) by scenario (drama) by study type (survey)	-2.109e+00	0.99960
code (back and forth) by scenario (drama) by study type (survey)	-1.605e+01	0.99588
code (communication control) by scenario (drama) by study type (survey)	-1.210e+00	0.21776
code (conditional reaction) by scenario (drama) by study type (survey)	1.647e+01	0.99458
code (nonreaction) by scenario (drama) by study type (survey)	1.631e+01	0.99512
code (exaggeration) by scenario (drama) by study type (survey)	-1.112e+00	0.99980
code (hurt reaction) by scenario (drama) by study type (survey)	-4.875e-02	0.96253
code (intent to hurt) by scenario (drama) by study type (survey)	-5.607e-01	0.52181
code (permanence) by scenario (drama) by study type (survey)	-5.535e-01	0.99988
code (permission) by scenario (drama) by study type (survey)	2.598e-01	0.86934
code (power imbalance) by scenario (drama) by study type (survey)	-3.917e-01	0.65672
code (repetition) by scenario (drama) by study type (survey)	2.999e-01	0.72204
code (serious harm) by scenario (drama) by study type (survey)	-8.755e-01	0.56023
participant (parent) by code (anger) by scenario (drama)	-1.807e+01	0.99577
participant (parent) by code (back and forth) by scenario (drama)	1.765e+01	0.99467
participant (parent) by code (communication control) by scenario (drama)	2.154e+00	0.02021 *
participant (parent) by code (conditional reaction) by scenario (drama)	-7.938e-01	0.60876
participant (parent) by code (nonreaction) by scenario (drama)	-1.947e-01	0.86141

participant (parent) by code (exaggeration) by scenario (drama)	5.928e-01	0.99989
participant (parent) by code (hurt reaction) by scenario (drama)	1.698e+00	0.07403 .
participant (parent) by code (intent to hurt) by scenario (drama)	-7.463e-01	0.34975
participant (parent) by code (permanence) by scenario (drama)	6.311e-01	0.73711
participant (parent) by code (permission) by scenario (drama)	-1.772e+01	0.99523
participant (parent) by code (power imbalance) by scenario (drama)	9.159e-02	0.91918
participant (parent) by code (repetition) by scenario (drama)	3.224e-01	0.70303
participant (parent) by code (serious harm) by scenario (drama)	-6.216e-01	0.67526

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Table E.3: Model of interview and survey participant qualitative coding data, which examines primarily interactions between the factors of participant age, code, scenario, and study type.

Appendix F

Online Safety Risks: Supplementary Tables

F.1 Models of Risk Likert Responses

F.1.1 Interview, Model 1: Entrance and Exit Data

Results of a linear mixed model fit by restricted maximum likelihood.

REML criterion at convergence by 15774.3

Scaled residuals:

Min	1Q	Median	3Q	Max
-4.0527	-0.5872	0.1268	0.6419	3.9187

Random effects:

Groups	Name	Variance	Std.Dev.
id	(Intercept)	0.05909	0.2431
Residual		0.92412	0.9613

Number of obs by 5636, groups by id, 31

Fixed Effects	Estimate	p
(Intercept)	1.38530	5.10e-10 ***
time (exit)	-0.11379	0.093598 .
condition (contract)	-0.07189	0.564986
condition (software)	-0.21254	0.082621 .
participant (parent)	0.47909	0.007524 **
child gender (female)	-0.08974	0.382849
child gender (other)	-0.21018	0.320468
parent gender (female)	-0.04694	0.762758
risk (being bullied)	0.93548	6.28e-08 ***
risk (bullies another)	0.03226	0.851798
risk (illegal downloads)	0.58065	0.000776 ***

risk (visits adult content)	0.11762	0.497522
risk (visits drug content)	0.08065	0.640458
risk (visits self harm content)	-0.08065	0.640458
risk (strained relationships)	0.35309	0.041732 *
risk (poor schoolwork)	0.46774	0.006768 **
risk (too little sleep)	1.16659	1.88e-11 ***
risk (contact by stranger)	0.91935	1.05e-07 ***
risk (texting and driving)	0.14516	0.400523
risk (viruses)	0.87097	4.69e-07 ***
evaluation (severity)	3.70785	< 2e-16 ***
evaluation (child prevention)	3.43383	< 2e-16 ***
evaluation (parent prevention)	3.27809	< 2e-16 ***
risk (being bullied) by evaluation (severity)	-1.49917	9.57e-10 ***
risk (bullies another) by evaluation (severity)	-0.38627	0.114467
risk (illegal downloads) by evaluation (severity)	-1.91852	5.33e-15 ***
risk (visits adult content) by evaluation (severity)	-0.72969	0.002931 **
risk (visits drug content) by evaluation (severity)	-0.57981	0.017836 *
risk (visits self harm content) by evaluation (severity)	-0.20885	0.393385
risk (strained relationships) by evaluation (severity)	-0.91677	0.000186 ***
risk (poor schoolwork) by evaluation (severity)	-1.01530	3.38e-05 ***
risk (too little sleep) by evaluation (severity)	-2.42382	< 2e-16 ***
risk (contact by stranger) by evaluation (severity)	-1.67659	8.06e-12 ***
risk (texting and driving) by evaluation (severity)	-0.74110	0.002466 **
risk (viruses) by evaluation (severity)	-1.62820	3.12e-11 ***
risk (being bullied) by evaluation (child prevention)	-1.82258	9.68e-14 ***
risk (bullies another) by evaluation (child prevention)	-0.12903	0.597211
risk (illegal downloads) by evaluation (child prevention)	-0.64516	0.008259 **
risk (visits adult content) by evaluation (child prevention)	-0.06923	0.777224
risk (visits drug content) by evaluation (child prevention)	-0.01613	0.947336
risk (visits self harm content) by evaluation (child prevention)	0.24194	0.321809
risk (strained relationships) by evaluation (child prevention)	-0.44147	0.071817 .
risk (poor schoolwork) by evaluation (child prevention)	-0.72581	0.002967 **
risk (too little sleep) by evaluation (child prevention)	-1.74723	1.05e-12 ***
risk (contact by stranger) by evaluation (child prevention)	-1.53226	3.76e-10 ***
risk (texting and driving) by evaluation (child prevention)	-0.14516	0.552201
risk (viruses) by evaluation (child prevention)	-1.62903	2.78e-11 ***
risk (being bullied) by evaluation (parent prevention)	-1.74194	1.10e-12 ***
risk (bullies another) by evaluation (parent prevention)	-0.33871	0.165446
risk (illegal downloads) by evaluation (parent prevention)	-1.16129	2.02e-06 ***
risk (visits adult content) by evaluation (parent prevention)	-0.52084	0.033322 *
risk (visits drug content) by evaluation (parent prevention)	-0.46774	0.055465 .
risk (visits self harm content) by evaluation (parent prevention)	-0.19355	0.428005
risk (strained relationships) by evaluation (parent prevention)	-0.57890	0.018017 *
risk (poor schoolwork) by evaluation (parent prevention)	-0.75806	0.001915 **
risk (too little sleep) by evaluation (parent prevention)	-1.55368	2.33e-10 ***
risk (contact by stranger) by evaluation (parent prevention)	-1.72581	1.77e-12 ***
risk (texting and driving) by evaluation (parent prevention)	-0.29032	0.234489
risk (viruses) by evaluation (parent prevention)	-1.48387	1.31e-09 ***
participant (parent) by risk (being bullied)	0.64516	0.008259 **
participant (parent) by risk (bullies another)	0.09677	0.691873
participant (parent) by risk (illegal downloads)	0.53226	0.029311 *
participant (parent) by risk (visits adult content)	1.20496	8.69e-07 ***
participant (parent) by risk (visits drug content)	0.82258	0.000760 ***
participant (parent) by risk (visits self harm content)	0.59677	0.014554 *
participant (parent) by risk (strained relationships)	0.75981	0.001910 **
participant (parent) by risk (poor schoolwork)	0.38710	0.112947

participant (parent) by risk (too little sleep)	0.39793	0.103931
participant (parent) by risk (contact by stranger)	-0.03226	0.894901
participant (parent) by risk (texting and driving)	0.30645	0.209510
participant (parent) by risk (viruses)	0.72581	0.002967 **
participant (parent) by evaluation (severity)	-0.65326	0.010085 *
participant (parent) by evaluation (parent prevention)	-1.66488	5.49e-11 ***
time (exit) by evaluation (severity)	0.19554	0.041482 *
time (exit) by evaluation (child prevention)	0.06783	0.479384
time (exit) by evaluation (parent prevention)	0.18575	0.052723 .
time (exit) by participant (parent)	0.04183	0.662637
participant (parent) by risk (being bullied) by evaluation (severity)	-0.56535	0.101997
participant (parent) by risk (bullies another) by evaluation (severity)	-0.14599	0.672787
participant (parent) by risk (illegal downloads) by evaluation (severity)	-0.92019	0.007789 **
participant (parent) by risk (visits adult content) by evaluation (severity)	-1.60902	3.40e-06 ***
participant (parent) by risk (visits drug content) by evaluation (severity)	-1.11373	0.001281 **
participant (parent) by risk (visits self harm content) by evaluation (severity)	-0.66212	0.055483 .
participant (parent) by risk (strained relationships) by evaluation (severity)	-1.01871	0.003253 **
participant (parent) by risk (poor schoolwork) by evaluation (severity)	-0.32341	0.349513
participant (parent) by risk (too little sleep) by evaluation (severity)	-0.17296	0.617209
participant (parent) by risk (contact by stranger) by evaluation (severity)	0.11207	0.745786
participant (parent) by risk (texting and driving) by evaluation (severity)	0.14433	0.676301
participant (parent) by risk (viruses) by evaluation (severity)	-1.58148	4.86e-06 ***
participant (parent) by risk (being bullied) by evaluation (parent prevention)	-1.00000	0.003795 **
participant (parent) by risk (bullies another) by evaluation (parent prevention)	0.09677	0.779295
participant (parent) by risk (illegal downloads) by evaluation (parent prevention)	-0.87097	0.011688 *
participant (parent) by risk (visits adult content) by evaluation (parent prevention)	-1.62432	2.68e-06 ***
participant (parent) by risk (visits drug content) by evaluation (parent prevention)	-1.22581	0.000389 ***
participant (parent) by risk (visits self harm content) by evaluation (parent prevention)	-1.03635	0.002729 **
participant (parent) by risk (strained relationships) by evaluation (parent prevention)	-0.43723	0.205963
participant (parent) by risk (poor schoolwork) by evaluation (parent prevention)	0.17742	0.607417
participant (parent) by risk (too little sleep) by evaluation (parent prevention)	0.19884	0.565150
participant (parent) by risk (contact by stranger) by evaluation (parent prevention)	0.20968	0.543736
participant (parent) by risk (texting and driving) by evaluation (parent prevention)	-0.24194	0.483565
participant (parent) by risk (viruses) by evaluation (parent prevention)	-0.91935	0.007781 **
time (exit) by participant (parent) by evaluation (severity)	0.27592	0.041810 *
time (exit) by participant (parent) by evaluation (parent prevention)	0.13621	0.314946
Signif. codes by 0 *** 0.001 ** 0.01 * 0.05 . 0.1 1		

Table F.1: Model of interview participant entrance and exit data, which examines primarily interactions between the factors of risk, participant age, and evaluation type.

F.1.2   Survey, Model 1: Entrance and Exit Data

Results of a linear mixed model fit by restricted maximum likelihood.

REML criterion at convergence by 55323.3

Scaled residuals:

Min	1Q	Median	3Q	Max
-3.4142	-0.6640	0.1497	0.7111	3.2471

Random effects:

Groups	Name	Variance	Std.Dev.
id	(Intercept)	0.1448	0.3805
Residual		1.5937	1.2624

Number of obs by 16604, groups by id, 79

Fixed effects	Estimate	p
(Intercept)	1.262e+00	2.07e-09 ***
time (exit)	-2.236e-01	0.000202 ***
condition (contract)	2.354e-01	0.064955 .
condition (software)	-7.729e-02	0.606602
condition (not yet assigned)	-1.864e-02	0.861656
participant (parent)	2.585e-01	0.124522
child gender (female)	1.126e-01	0.234793
child gender (other)	-1.404e-01	0.728732
parent gender (female)	-2.837e-02	0.853479
parent gender (other)	1.847e-01	0.668050
parent gender (decline to answer)	-2.217e-01	0.598495
risk (accidental adult content)	5.664e-01	0.000618 ***
risk (accidental drug content)	5.313e-01	0.001352 **
risk (accidental self harm content)	2.997e-01	0.070617 .
risk (online ads)	2.493e+00	< 2e-16 ***
risk (being bullied)	7.117e-01	1.70e-05 ***
risk (bullies another)	6.211e-02	0.707280
risk (illegal downloads)	5.151e-01	0.001848 **
risk (strained relationships)	6.262e-01	0.000154 ***
risk (poor schoolwork)	4.040e-01	0.014601 *
risk (seeks adult content)	2.715e-01	0.101512
risk (seeks drug content)	1.263e-01	0.446307
risk (seeks self harm content)	1.083e-02	0.947787
risk (too little sleep)	1.002e+00	1.40e-09 ***
risk (contact by stranger)	8.989e-01	5.96e-08 ***
risk (texting and driving)	9.941e-02	0.549591
risk (too much time online)	1.404e+00	< 2e-16 ***
risk (viruses)	7.715e-01	3.12e-06 ***
evaluation (severity)	2.918e+00	< 2e-16 ***
evaluation (child prevention)	2.661e+00	< 2e-16 ***
evaluation (parent prevention)	2.943e+00	< 2e-16 ***
risk (accidental adult content) by evaluation (severity)	-1.159e+00	7.79e-07 ***
risk (accidental drug content) by evaluation (severity)	-1.077e+00	4.52e-06 ***
risk (accidental self harm content) by evaluation (severity)	-5.842e-01	0.012711 *
risk (online ads) by evaluation (severity)	-4.656e+00	< 2e-16 ***
risk (being bullied) by evaluation (severity)	-1.108e+00	2.24e-06 ***
risk (bullies another) by evaluation (severity)	-3.035e-01	0.194986
risk (illegal downloads) by evaluation (severity)	-1.317e+00	1.90e-08 ***
risk (strained relationships) by evaluation (severity)	-1.290e+00	3.67e-08 ***
risk (poor schoolwork) by evaluation (severity)	-1.004e+00	1.77e-05 ***
risk (seeks adult content) by evaluation (severity)	-8.232e-01	0.000447 ***
risk (seeks drug content) by evaluation (severity)	-4.021e-01	0.086308 .
risk (seeks self harm content) by evaluation (severity)	-1.832e-01	0.433918
risk (too little sleep) by evaluation (severity)	-1.891e+00	8.23e-16 ***
risk (contact by stranger) by evaluation (severity)	-1.539e+00	5.59e-11 ***
risk (texting and driving) by evaluation (severity)	-4.898e-01	0.037085 *

risk (time) by evaluation (severity)	-2.654e+00	< 2e-16 ***
risk (viruses) by evaluation (severity)	-1.556e+00	3.14e-11 ***
risk (accidental adult content) by evaluation (child prevention)	-7.043e-01	0.002636 **
risk (accidental drug content) by evaluation (child prevention)	-6.262e-01	0.007569 **
risk (accidental self harm content) by evaluation (child prevention)	-3.256e-01	0.164907
risk (online ads) by evaluation (child prevention)	-3.717e+00	< 2e-16 ***
risk (being bullied) by evaluation (child prevention)	-1.091e+00	3.20e-06 ***
risk (bullies another) by evaluation (child prevention)	2.137e-01	0.361372
risk (illegal downloads) by evaluation (child prevention)	-5.065e-01	0.030566 *
risk (strained relationships) by evaluation (child prevention)	-6.779e-01	0.003796 **
risk (poor schoolwork) by evaluation (child prevention)	-3.695e-01	0.114598
risk (seeks adult content) by evaluation (child prevention)	-9.432e-02	0.687771
risk (seeks drug content) by evaluation (child prevention)	6.341e-02	0.786792
risk (seeks self harm content) by evaluation (child prevention)	1.945e-01	0.406797
risk (too little sleep) by evaluation (child prevention)	-1.235e+00	1.35e-07 ***
risk (contact by stranger) by evaluation (child prevention)	-1.451e+00	6.25e-10 ***
risk (texting and driving) by evaluation (child prevention)	2.919e-01	0.214004
risk (time) by evaluation (child prevention)	-1.568e+00	2.23e-11 ***
risk (viruses) by evaluation (child prevention)	-1.245e+00	1.10e-07 ***
risk (accidental adult content) by evaluation (parent prevention)	-8.161e-01	0.000501 ***
risk (accidental drug content) by evaluation (parent prevention)	-7.709e-01	0.001050 **
risk (accidental self harm content) by evaluation (parent prevention)	-3.919e-01	0.094956 .
risk (online ads) by evaluation (parent prevention)	-3.820e+00	< 2e-16 ***
risk (being bullied) by evaluation (parent prevention)	-9.617e-01	4.03e-05 ***
risk (bullies another) by evaluation (parent prevention)	-9.452e-02	0.687131
risk (illegal downloads) by evaluation (parent prevention)	-8.689e-01	0.000211 ***
risk (strained relationships) by evaluation (parent prevention)	-7.942e-01	0.000706 ***
risk (poor schoolwork) by evaluation (parent prevention)	-4.471e-01	0.056245 .
risk (seeks adult content) by evaluation (parent prevention)	-3.491e-01	0.136512
risk (seeks drug content) by evaluation (parent prevention)	-2.038e-01	0.385146
risk (seeks self harm content) by evaluation (parent prevention)	-1.184e-01	0.613415
risk (too little sleep) by evaluation (parent prevention)	-1.140e+00	1.13e-06 ***
risk (contact by stranger) by evaluation (parent prevention)	-1.361e+00	6.80e-09 ***
risk (texting and driving) by evaluation (parent prevention)	-1.362e-02	0.953769
risk (time) by evaluation (parent prevention)	-1.556e+00	3.42e-11 ***
risk (viruses) by evaluation (parent prevention)	-1.194e+00	3.46e-07 ***
participant (parent) by risk (accidental adult content)	8.162e-01	0.000507 ***
participant (parent) by risk (accidental drug content)	6.252e-01	0.007795 **
participant (parent) by risk (accidental self harm content)	2.324e-01	0.323143
participant (parent) by risk (online ads)	3.770e-01	0.108567
participant (parent) by risk (being bullied)	5.753e-01	0.014246 *
participant (parent) by risk (bullies another)	3.354e-02	0.886364
participant (parent) by risk (illegal downloads)	2.501e-01	0.286554
participant (parent) by risk (strained relationships)	2.434e-01	0.299785
participant (parent) by risk (poor schoolwork)	4.395e-01	0.061131 .
participant (parent) by risk (seeks adult content)	3.459e-01	0.140924
participant (parent) by risk (seeks drug content)	5.636e-02	0.810408
participant (parent) by risk (seeks self harm content)	-1.953e-02	0.933686
participant (parent) by risk (too little sleep)	3.195e-01	0.173463
participant (parent) by risk (contact by stranger)	1.359e-01	0.562879
participant (parent) by risk (texting and driving)	-3.929e-02	0.867485
participant (parent) by risk (too much time online)	6.569e-01	0.005132 **
participant (parent) by risk (viruses)	6.401e-01	0.006442 **
participant (parent) by evaluation (severity)	9.724e-02	0.682800
participant (parent) by evaluation (child prevention)	-3.907e-01	0.100710
participant (parent) by evaluation (parent prevention)	-8.776e-01	0.000231 ***

time (exit) by evaluation (severity)	2.907e-01	0.000507 ***
time (exit) by evaluation (child prevention)	1.097e-01	0.187591
time (exit) by evaluation (parent prevention)	6.443e-02	0.439696
time (exit) by participant (parent)	4.073e-02	0.628032
participant (parent) by risk (accidental adult content) by evaluation (severity)	-6.978e-01	0.035831 *
participant (parent) by risk (accidental drug content) by evaluation (severity)	-4.538e-01	0.172212
participant (parent) by risk (accidental self harm content) by evaluation (severity)	-1.827e-01	0.582642
participant (parent) by risk (online ads) by evaluation (severity)	-2.915e-01	0.380335
participant (parent) by risk (being bullied) by evaluation (severity)	-3.091e-01	0.351869
participant (parent) by risk (bullies another) by evaluation (severity)	1.219e-01	0.713643
participant (parent) by risk (illegal downloads) by evaluation (severity)	-4.484e-01	0.176940
participant (parent) by risk (strained relationships) by evaluation (severity)	-1.274e-01	0.701278
participant (parent) by risk (poor schoolwork) by evaluation (severity)	-1.175e-01	0.723357
participant (parent) by risk (seeks adult content) by evaluation (severity)	-1.681e-01	0.612870
participant (parent) by risk (seeks drug content) by evaluation (severity)	-6.746e-02	0.839113
participant (parent) by risk (seeks self harm content) by evaluation (severity)	9.629e-02	0.771843
participant (parent) by risk (too little sleep) by evaluation (severity)	3.000e-01	0.366786
participant (parent) by risk (contact by stranger) by evaluation (severity)	2.435e-01	0.463829
participant (parent) by risk (texting and driving) by evaluation (severity)	4.297e-01	0.196631
participant (parent) by risk (time) by evaluation (severity)	-2.069e-01	0.533298
participant (parent) by risk (viruses) by evaluation (severity)	-1.012e+00	0.002319 **
participant (parent) by risk (accidental adult content) by evaluation (child prevention)	-1.410e+00	2.20e-05 ***
participant (parent) by risk (accidental drug content) by evaluation (child prevention)	-1.035e+00	0.001847 **
participant (parent) by risk (accidental self harm content) by evaluation (child prevention)	-5.717e-01	0.085472 .
participant (parent) by risk (online ads) by evaluation (child prevention)	-7.355e-01	0.026865 *
participant (parent) by risk (being bullied) by evaluation (child prevention)	-1.001e+00	0.002601 **
participant (parent) by risk (bullies another) by evaluation (child prevention)	-2.586e-01	0.436313
participant (parent) by risk (illegal downloads) by evaluation (child prevention)	-6.848e-01	0.039195 *
participant (parent) by risk (strained relationships) by evaluation (child prevention)	-7.655e-01	0.021158 *
participant (parent) by risk (poor schoolwork) by evaluation (child prevention)	-8.218e-01	0.013342 *
participant (parent) by risk (seeks adult content) by evaluation (child prevention)	-8.187e-01	0.013792 *
participant (parent) by risk (seeks drug content) by evaluation (child prevention)	-3.885e-01	0.242504
participant (parent) by risk (seeks self harm content) by evaluation (child prevention)	-1.510e-01	0.649498
participant (parent) by risk (too little sleep) by evaluation (child prevention)	-6.954e-01	0.036264 *
participant (parent) by risk (contact by stranger) by evaluation (child prevention)	-2.364e-01	0.476810
participant (parent) by risk (texting and driving) by evaluation (child prevention)	-4.216e-01	0.205180
participant (parent) by risk (time) by evaluation (child prevention)	-1.537e+00	3.73e-06 ***
participant (parent) by risk (viruses) by evaluation (child prevention)	-1.219e+00	0.000247 ***
participant (parent) by risk (accidental adult content) by evaluation (parent prevention)	-1.386e+00	3.10e-05 ***
participant (parent) by risk (accidental drug content) by evaluation (parent prevention)	-9.806e-01	0.003235 **
participant (parent) by risk (accidental self harm content) by evaluation (parent prevention)	-5.438e-01	0.102241
participant (parent) by risk (online ads) by evaluation (parent prevention)	-8.444e-01	0.011094 *
participant (parent) by risk (being bullied) by evaluation (parent prevention)	-1.320e+00	7.11e-05 ***
participant (parent) by risk (bullies another) by evaluation (parent prevention)	5.457e-02	0.869743
participant (parent) by risk (illegal downloads) by evaluation (parent prevention)	-3.782e-01	0.255279
participant (parent) by risk (strained relationships) by evaluation (parent prevention)	-3.573e-01	0.282506
participant (parent) by risk (poor schoolwork) by evaluation (parent prevention)	-4.522e-01	0.173527
participant (parent) by risk (seeks adult content) by evaluation (parent prevention)	-7.068e-01	0.033513 *

194

participant (parent) by risk (seeks drug content) by evaluation (parent prevention)	-2.024e-01	0.542986
participant (parent) by risk (seeks self harm content) by evaluation (parent prevention)	-4.173e-02	0.900106
participant (parent) by risk (too little sleep) by evaluation (parent prevention)	-2.373e-01	0.475024
participant (parent) by risk (contact by stranger) by evaluation (parent prevention)	-4.341e-01	0.191909
participant (parent) by risk (texting and driving) by evaluation (parent prevention)	-2.406e-02	0.942398
participant (parent) by risk (time) by evaluation (parent prevention)	-9.689e-01	0.003584 **
participant (parent) by risk (viruses) by evaluation (parent prevention)	-1.117e+00	0.000781 ***
time (exit) by participant (parent) by evaluation (severity)	-3.684e-01	0.001961 **
time (exit) by participant (parent) by evaluation (child prevention)	1.650e-01	0.164587
time (exit) by participant (parent) by evaluation (parent prevention)	4.040e-01	0.000675 ***
Signif. codes by 0 *** 0.001 ** 0.01 * 0.05 . 0.1 1		

Table F.2: Model of survey participant entrance and exit data, which examines primarily interactions between the factors of risk, participant age, and evaluation type.

F.1.3   Interview, Model 2: Exit Data Only

Results of a linear mixed model fit by restricted maximum likelihood.

REML criterion at convergence by 7703.3

Scaled residuals:

Min	1Q	Median	3Q	Max
-3.7669	-0.5711	0.1153	0.5787	4.3124

Random effects:

Groups	Name	Variance	Std.Dev.
id	(Intercept)	0.0489	0.2211
Residual		0.8723	0.9340

Number of obs by 2818, groups by id, 31

Fixed Effects	Estimate	p
(Intercept)	9.643e-01	0.000210 ***
condition (contract)	-1.206e-01	0.710982
condition (software)	1.158e-01	0.714830
participant (parent)	8.846e-01	3.11e-14 ***
child gender (female)	-1.443e-02	0.882276
child gender (other)	-1.961e-01	0.331344
parent gender (female)	-1.140e-01	0.444742
risk (being bullied)	1.050e+00	0.000384 ***
risk (bullies another)	-7.217e-14	1.000000
risk (illegal downloads)	8.000e-01	0.006798 **
risk (visits adult content)	6.000e-01	0.042301 *
risk (visits drug content)	4.000e-01	0.175738
risk (visits self harm content)	2.000e-01	0.498351

risk (strained relationships)	3.000e-01	0.309832
risk (poor schoolwork)	1.500e-01	0.611576
risk (too little sleep)	1.000e+00	0.000720 ***
risk (contact by stranger)	5.000e-01	0.090583 .
risk (texting and driving)	-5.000e-02	0.865577
risk (viruses)	9.000e-01	0.002332 **
evaluation (severity)	4.057e+00	< 2e-16 ***
evaluation (child prevention)	4.042e+00	< 2e-16 ***
evaluation (parent prevention)	4.054e+00	< 2e-16 ***
risk (being bullied) by evaluation (severity)	-1.392e+00	0.000944 ***
risk (bullies another) by evaluation (severity)	-2.419e-01	0.565134
risk (illegal downloads) by evaluation (severity)	-1.992e+00	2.28e-06 ***
risk (visits adult content) by evaluation (severity)	-1.042e+00	0.013274 *
risk (visits drug content) by evaluation (severity)	-7.919e-01	0.059753 .
risk (visits self harm content) by evaluation (severity)	-4.419e-01	0.293362
risk (strained relationships) by evaluation (severity)	-7.919e-01	0.059753 .
risk (poor schoolwork) by evaluation (severity)	-3.419e-01	0.416209
risk (too little sleep) by evaluation (severity)	-1.792e+00	2.10e-05 ***
risk (contact by stranger) by evaluation (severity)	-8.919e-01	0.033993 *
risk (texting and driving) by evaluation (severity)	-2.919e-01	0.487602
risk (viruses) by evaluation (severity)	-1.942e+00	4.05e-06 ***
risk (being bullied) by evaluation (child prevention)	-1.950e+00	0.000141 ***
risk (bullies another) by evaluation (child prevention)	-4.000e-01	0.434320
risk (illegal downloads) by evaluation (child prevention)	-9.000e-01	0.078632 .
risk (visits adult content) by evaluation (child prevention)	-6.000e-01	0.240938
risk (visits drug content) by evaluation (child prevention)	-4.000e-01	0.434320
risk (visits self harm content) by evaluation (child prevention)	-2.000e-01	0.695851
risk (strained relationships) by evaluation (child prevention)	-6.000e-01	0.240938
risk (poor schoolwork) by evaluation (child prevention)	-1.500e-01	0.769371
risk (too little sleep) by evaluation (child prevention)	-1.500e+00	0.003394 **
risk (contact by stranger) by evaluation (child prevention)	-1.000e+00	0.050706 .
risk (texting and driving) by evaluation (child prevention)	-1.500e-01	0.769371
risk (viruses) by evaluation (child prevention)	-1.800e+00	0.000441 ***
risk (being bullied) by evaluation (parent prevention)	-1.800e+00	1.70e-05 ***
risk (bullies another) by evaluation (parent prevention)	2.169e-13	1.000000
risk (illegal downloads) by evaluation (parent prevention)	-1.300e+00	0.001875 **
risk (visits adult content) by evaluation (parent prevention)	-1.250e+00	0.002791 **
risk (visits drug content) by evaluation (parent prevention)	-1.050e+00	0.012000 *
risk (visits self harm content) by evaluation (parent prevention)	-8.000e-01	0.055556 .
risk (strained relationships) by evaluation (parent prevention)	-1.000e-01	0.810799
risk (poor schoolwork) by evaluation (parent prevention)	5.000e-02	0.904722
risk (too little sleep) by evaluation (parent prevention)	-9.000e-01	0.031270 *
risk (contact by stranger) by evaluation (parent prevention)	-9.000e-01	0.031270 *
risk (texting and driving) by evaluation (parent prevention)	4.000e-01	0.338313
risk (viruses) by evaluation (parent prevention)	-1.250e+00	0.002791 **
condition (contract) by risk (being bullied)	3.500e-01	0.402125
condition (software) by risk (being bullied)	-4.545e-03	0.991114
condition (contract) by risk (bullies another)	1.500e-01	0.719527
condition (software) by risk (bullies another)	-4.545e-02	0.911317
condition (contract) by risk (illegal downloads)	1.500e-01	0.719527
condition (software) by risk (illegal downloads)	1.818e-02	0.964465
condition (contract) by risk (visits adult content)	5.000e-02	0.904722
condition (software) by risk (visits adult content)	3.091e-01	0.448855
condition (contract) by risk (visits drug content)	1.500e-01	0.719527
condition (software) by risk (visits drug content)	1.000e-01	0.806434
condition (contract) by risk (visits self harm content)	5.000e-02	0.904722

condition (software) by risk (visits self harm content)	2.727e-02	0.946720
condition (contract) by risk (strained relationships)	6.500e-01	0.119775
condition (software) by risk (strained relationships)	5.636e-01	0.167331
condition (contract) by risk (poor schoolwork)	7.500e-01	0.072666 .
condition (software) by risk (poor schoolwork)	7.136e-01	0.080444 .
condition (contract) by risk (too little sleep)	5.000e-01	0.231377
condition (software) by risk (too little sleep)	5.354e-01	0.192150
condition (contract) by risk (contact by stranger)	3.500e-01	0.402125
condition (software) by risk (contact by stranger)	9.545e-01	0.019402 *
condition (contract) by risk (texting and driving)	4.500e-01	0.281406
condition (software) by risk (texting and driving)	3.682e-01	0.367010
condition (contract) by risk (viruses)	3.500e-01	0.402125
condition (software) by risk (viruses)	4.182e-01	0.305566
condition (contract) by evaluation (severity)	2.434e-01	0.577267
condition (software) by evaluation (severity)	-9.783e-02	0.818653
condition (contract) by evaluation (child prevention)	1.577e-01	0.760857
condition (software) by evaluation (child prevention)	-8.317e-01	0.100455
condition (contract) by evaluation (parent prevention)	-6.038e-01	0.163697
condition (software) by evaluation (parent prevention)	-6.818e-01	0.107531
participant (parent) by evaluation (severity)	-8.295e-01	4.52e-07 ***
participant (parent) by evaluation (parent prevention)	-2.308e+00	< 2e-16 ***
condition (contract) by participant (parent)	3.154e-01	0.054323 .
condition (software) by participant (parent)	8.196e-02	0.608949
condition (contract) by risk (being bullied) by evaluation (severity)	-4.081e-01	0.491121
condition (software) by risk (being bullied) by evaluation (severity)	-1.536e-01	0.790896
condition (contract) by risk (bullies another) by evaluation (severity)	-2.081e-01	0.725500
condition (software) by risk (bullies another) by evaluation (severity)	-1.217e-01	0.833503
condition (contract) by risk (illegal downloads) by evaluation (severity)	-5.081e-01	0.391326
condition (software) by risk (illegal downloads) by evaluation (severity)	-5.081e-01	0.380353
condition (contract) by risk (visits adult content) by evaluation (severity)	-3.581e-01	0.545725
condition (software) by risk (visits adult content) by evaluation (severity)	-6.854e-01	0.236716
condition (contract) by risk (visits drug content) by evaluation (severity)	-1.581e-01	0.789653
condition (software) by risk (visits drug content) by evaluation (severity)	-3.899e-01	0.500802
condition (contract) by risk (visits self harm content) by evaluation (severity)	-8.112e-03	0.989080
condition (software) by risk (visits self harm content) by evaluation (severity)	-1.036e-01	0.858080
condition (contract) by risk (strained relationships) by evaluation (severity)	-6.581e-01	0.266903
condition (software) by risk (strained relationships) by evaluation (severity)	-8.445e-01	0.144900
condition (contract) by risk (poor schoolwork) by evaluation (severity)	-1.058e+00	0.074313 .
condition (software) by risk (poor schoolwork) by evaluation (severity)	-1.204e+00	0.037780 *
condition (contract) by risk (too little sleep) by evaluation (severity)	-7.081e-01	0.232263
condition (software) by risk (too little sleep) by evaluation (severity)	-1.062e+00	0.067644 .
condition (contract) by risk (contact by stranger) by evaluation (severity)	-3.581e-01	0.545725
condition (software) by risk (contact by stranger) by evaluation (severity)	-1.608e+00	0.005528 **
condition (contract) by risk (texting and driving) by evaluation (severity)	-4.081e-01	0.491121
condition (software) by risk (texting and driving) by evaluation (severity)	-4.354e-01	0.452232
condition (contract) by risk (viruses) by evaluation (severity)	-2.081e-01	0.725500
condition (software) by risk (viruses) by evaluation (severity)	-5.581e-01	0.335268
condition (contract) by risk (being bullied) by evaluation (child prevention)	-4.500e-01	0.533976
condition (software) by risk (being bullied) by evaluation (child prevention)	-9.545e-02	0.892582
condition (contract) by risk (bullies another) by evaluation (child prevention)	-5.000e-02	0.944904
condition (software) by risk (bullies another) by evaluation (child prevention)	7.182e-01	0.309677
condition (contract) by risk (illegal downloads) by evaluation (child prevention)	-3.500e-01	0.628567
condition (software) by risk (illegal downloads) by evaluation (child prevention)	1.727e-01	0.806957
condition (contract) by risk (visits adult content) by evaluation (child prevention)	-3.500e-01	0.628567
condition (software) by risk (visits adult content) by evaluation (child prevention)	-3.091e-01	0.661924
condition (contract) by risk (visits drug content) by evaluation (child prevention)	-4.500e-01	0.533976

condition (software) by risk (visits drug content) by evaluation (child prevention)	8.182e-02	0.907853
condition (contract) by risk (visits self harm content) by evaluation (child prevention)	-1.500e-01	0.835758
condition (software) by risk (visits self harm content) by evaluation (child prevention)	1.545e-01	0.826937
condition (contract) by risk (strained relationships) by evaluation (child prevention)	-6.500e-01	0.369008
condition (software) by risk (strained relationships) by evaluation (child prevention)	-1.727e-01	0.806957
condition (contract) by risk (poor schoolwork) by evaluation (child prevention)	-1.250e+00	0.084131 .
condition (software) by risk (poor schoolwork) by evaluation (child prevention)	-1.077e+00	0.127593
condition (contract) by risk (too little sleep) by evaluation (child prevention)	-8.000e-01	0.268901
condition (software) by risk (too little sleep) by evaluation (child prevention)	-8.536e-01	0.228167
condition (contract) by risk (contact by stranger) by evaluation (child prevention)	-5.500e-01	0.447168
condition (software) by risk (contact by stranger) by evaluation (child prevention)	-1.545e+00	0.028864 *
condition (contract) by risk (texting and driving) by evaluation (child prevention)	-3.500e-01	0.628567
condition (software) by risk (texting and driving) by evaluation (child prevention)	-7.727e-02	0.912952
condition (contract) by risk (viruses) by evaluation (child prevention)	-3.500e-01	0.628567
condition (software) by risk (viruses) by evaluation (child prevention)	1.182e-01	0.867221
condition (contract) by risk (being bullied) by evaluation (parent prevention)	-7.000e-01	0.236098
condition (software) by risk (being bullied) by evaluation (parent prevention)	2.727e-02	0.962311
condition (contract) by risk (bullies another) by evaluation (parent prevention)	-3.000e-01	0.611576
condition (software) by risk (bullies another) by evaluation (parent prevention)	-3.182e-01	0.581446
condition (contract) by risk (illegal downloads) by evaluation (parent prevention)	-1.000e-01	0.865577
condition (software) by risk (illegal downloads) by evaluation (parent prevention)	-5.182e-01	0.369321
condition (contract) by risk (visits adult content) by evaluation (parent prevention)	3.000e-01	0.611576
condition (software) by risk (visits adult content) by evaluation (parent prevention)	-3.409e-01	0.554756
condition (contract) by risk (visits drug content) by evaluation (parent prevention)	3.500e-01	0.553545
condition (software) by risk (visits drug content) by evaluation (parent prevention)	-8.636e-02	0.881052
condition (contract) by risk (visits self harm content) by evaluation (parent prevention)	4.000e-01	0.498351
condition (software) by risk (visits self harm content) by evaluation (parent prevention)	1.912e-02	0.973643
condition (contract) by risk (strained relationships) by evaluation (parent prevention)	-8.000e-01	0.175738
condition (software) by risk (strained relationships) by evaluation (parent prevention)	-1.036e+00	0.072641 .
condition (contract) by risk (poor schoolwork) by evaluation (parent prevention)	-7.000e-01	0.236098
condition (software) by risk (poor schoolwork) by evaluation (parent prevention)	-1.050e+00	0.068960 .
condition (contract) by risk (too little sleep) by evaluation (parent prevention)	-6.000e-01	0.309832
condition (software) by risk (too little sleep) by evaluation (parent prevention)	-7.263e-01	0.209602
condition (contract) by risk (contact by stranger) by evaluation (parent prevention)	-8.500e-01	0.150267
condition (software) by risk (contact by stranger) by evaluation (parent prevention)	-1.327e+00	0.021533 *
condition (contract) by risk (texting and driving) by evaluation (parent prevention)	-2.500e-01	0.672156
condition (software) by risk (texting and driving) by evaluation (parent prevention)	-1.173e+00	0.042245 *
condition (contract) by risk (viruses) by evaluation (parent prevention)	-7.000e-01	0.236098
condition (software) by risk (viruses) by evaluation (parent prevention)	-9.318e-01	0.106507
condition (contract) by participant (parent) by evaluation (severity)	-4.705e-01	0.042494 *
condition (software) by participant (parent) by evaluation (severity)	2.801e-03	0.990136
condition (contract) by participant (parent) by evaluation (parent prevention)	4.077e-01	0.078578 .
condition (software) by participant (parent) by evaluation (parent prevention)	3.818e-01	0.092051 .

Signif. codes by 0 *** 0.001 ** 0.01 * 0.05 . 0.1   1

Table F.3: Model of interview participant exit data only, which examines primarily interactions between the factors of study condition, risk, participant age, and evaluation type.

F.1.4 Survey, Model 2: Exit Data Only

Results of a linear mixed model fit by restricted maximum likelihood.

REML criterion at convergence by 17256.4

Scaled residuals:

Min	1Q	Median	3Q	Max
-3.2553	-0.6530	0.1441	0.6816	3.4223

Random effects:

Groups	Name	Variance	Std.Dev.
id	(Intercept)	0.3409	0.5839
Residual		1.4812	1.2171

Number of obs by 5301, groups by id, 39

Fixed Effects	Estimate	p
(Intercept)	1.439e+00	0.002475 **
condition (contract)	4.881e-02	0.911750
condition (software)	-2.318e-03	0.995688
participant (parent)	4.654e-01	0.000114 ***
child gender (female)	-2.850e-01	0.164044
parent gender (female)	-3.538e-01	0.344635
parent gender (other)	-2.620e-01	0.719806
parent gender (decline to answer)	-3.875e-01	0.591091
risk (accidental adult content)	1.043e+00	0.003659 **
risk (accidental drug content)	9.565e-01	0.007719 **
risk (accidental self harm content)	2.178e-01	0.548597
risk (online ads)	2.783e+00	1.08e-14 ***
risk (being bullied)	1.565e+00	1.32e-05 ***
risk (bullies another)	1.304e-01	0.716294
risk (illegal downloads)	4.783e-01	0.182723
risk (strained relationships)	9.565e-01	0.007719 **
risk (poor schoolwork)	5.652e-01	0.115344
risk (seeks adult content)	3.478e-01	0.332509
risk (seeks drug content)	8.696e-02	0.808564
risk (seeks self harm content)	1.304e-01	0.716294
risk (too little sleep)	1.696e+00	2.37e-06 ***
risk (contact by stranger)	1.043e+00	0.003659 **
risk (texting and driving)	-1.739e-01	0.627993
risk (too much time online)	2.087e+00	6.44e-09 ***
risk (viruses)	9.130e-01	0.010987 *
evaluation (severity)	2.964e+00	9.88e-16 ***
evaluation (child prevention)	2.724e+00	1.54e-13 ***

evaluation (parent prevention)	2.513e+00	9.54e-12 ***
risk (accidental adult content) by evaluation (severity)	-1.280e+00	0.012195 *
risk (accidental drug content) by evaluation (severity)	-1.043e+00	0.039843 *
risk (accidental self harm content) by evaluation (severity)	-3.482e-01	0.495193
risk (online ads) by evaluation (severity)	-4.739e+00	< 2e-16 ***
risk (being bullied) by evaluation (severity)	-1.609e+00	0.001536 **
risk (bullies another) by evaluation (severity)	-1.304e-01	0.797198
risk (illegal downloads) by evaluation (severity)	-1.000e+00	0.048865 *
risk (strained relationships) by evaluation (severity)	-1.261e+00	0.013016 *
risk (poor schoolwork) by evaluation (severity)	-6.522e-01	0.198871
risk (seeks adult content) by evaluation (severity)	-6.087e-01	0.230475
risk (seeks drug content) by evaluation (severity)	-2.174e-01	0.668440
risk (seeks self harm content) by evaluation (severity)	-8.696e-02	0.863974
risk (too little sleep) by evaluation (severity)	-2.014e+00	8.04e-05 ***
risk (contact by stranger) by evaluation (severity)	-9.987e-01	0.050469 .
risk (texting and driving) by evaluation (severity)	1.739e-01	0.731875
risk (time) by evaluation (severity)	-2.609e+00	2.85e-07 ***
risk (viruses) by evaluation (severity)	-1.783e+00	0.000448 ***
risk (accidental adult content) by evaluation (child prevention)	-1.565e+00	0.002054 **
risk (accidental drug content) by evaluation (child prevention)	-1.174e+00	0.020768 *
risk (accidental self harm content) by evaluation (child prevention)	-6.960e-01	0.172777
risk (online ads) by evaluation (child prevention)	-3.913e+00	1.51e-14 ***
risk (being bullied) by evaluation (child prevention)	-2.304e+00	5.75e-06 ***
risk (bullies another) by evaluation (child prevention)	-8.696e-02	0.863974
risk (illegal downloads) by evaluation (child prevention)	-6.957e-01	0.170559
risk (strained relationships) by evaluation (child prevention)	-1.130e+00	0.025975 *
risk (poor schoolwork) by evaluation (child prevention)	-9.565e-01	0.059543 .
risk (seeks adult content) by evaluation (child prevention)	-5.217e-01	0.304020
risk (seeks drug content) by evaluation (child prevention)	-2.609e-01	0.607290
risk (seeks self harm content) by evaluation (child prevention)	-3.043e-01	0.548773
risk (too little sleep) by evaluation (child prevention)	-2.304e+00	5.75e-06 ***
risk (contact by stranger) by evaluation (child prevention)	-1.739e+00	0.000616 ***
risk (texting and driving) by evaluation (child prevention)	3.478e-01	0.493184
risk (time) by evaluation (child prevention)	-2.652e+00	1.81e-07 ***
risk (viruses) by evaluation (child prevention)	-1.913e+00	0.000166 ***
risk (accidental adult content) by evaluation (parent prevention)	-1.304e+00	0.010202 *
risk (accidental drug content) by evaluation (parent prevention)	-1.086e+00	0.034581 *
risk (accidental self harm content) by evaluation (parent prevention)	-3.047e-01	0.550570
risk (online ads) by evaluation (parent prevention)	-4.000e+00	3.95e-15 ***
risk (being bullied) by evaluation (parent prevention)	-2.087e+00	3.99e-05 ***
risk (bullies another) by evaluation (parent prevention)	4.348e-02	0.931738
risk (illegal downloads) by evaluation (parent prevention)	-6.957e-01	0.170559
risk (strained relationships) by evaluation (parent prevention)	-7.557e-01	0.138819
risk (poor schoolwork) by evaluation (parent prevention)	-2.609e-01	0.607290
risk (seeks adult content) by evaluation (parent prevention)	-3.043e-01	0.548773
risk (seeks drug content) by evaluation (parent prevention)	-1.739e-01	0.731875
risk (seeks self harm content) by evaluation (parent prevention)	-2.174e-01	0.668440
risk (too little sleep) by evaluation (parent prevention)	-1.522e+00	0.002729 **
risk (contact by stranger) by evaluation (parent prevention)	-1.261e+00	0.013016 *
risk (texting and driving) by evaluation (parent prevention)	5.217e-01	0.304020
risk (time) by evaluation (parent prevention)	-2.211e+00	1.50e-05 ***
risk (viruses) by evaluation (parent prevention)	-1.217e+00	0.016496 *
condition (contract) by risk (accidental adult content)	-1.739e-01	0.731875
condition (software) by risk (accidental adult content)	-4.348e-02	0.928478
condition (contract) by risk (accidental drug content)	4.348e-02	0.931738
condition (software) by risk (accidental drug content)	-2.422e-01	0.617017
condition (contract) by risk (accidental self harm content)	3.909e-01	0.443791

condition (software) by risk (accidental self harm content)	-3.471e-03	0.994319
condition (contract) by risk (online ads)	2.609e-01	0.607290
condition (software) by risk (online ads)	-4.612e-01	0.341072
condition (contract) by risk (being bullied)	-7.826e-01	0.123153
condition (software) by risk (being bullied)	-8.509e-01	0.079011 .
condition (contract) by risk (bullies another)	-4.070e-14	1.000000
condition (software) by risk (bullies another)	-1.304e-01	0.787716
condition (contract) by risk (illegal downloads)	6.087e-01	0.230475
condition (software) by risk (illegal downloads)	-2.283e-01	0.637475
condition (contract) by risk (strained relationships)	-3.043e-01	0.548773
condition (software) by risk (strained relationships)	-5.637e-01	0.244590
condition (contract) by risk (poor schoolwork)	8.696e-02	0.863974
condition (software) by risk (poor schoolwork)	-2.438e-01	0.614762
condition (contract) by risk (seeks adult content)	-1.739e-01	0.731875
condition (software) by risk (seeks adult content)	-9.783e-02	0.839949
condition (contract) by risk (seeks drug content)	2.174e-01	0.668440
condition (software) by risk (seeks drug content)	-1.227e-01	0.800076
condition (contract) by risk (seeks self harm content)	-8.696e-02	0.863974
condition (software) by risk (seeks self harm content)	-2.376e-01	0.623804
condition (contract) by risk (too little sleep)	-9.130e-01	0.072091 .
condition (software) by risk (too little sleep)	-9.814e-01	0.042807 *
condition (contract) by risk (contact by stranger)	-2.609e-01	0.607290
condition (software) by risk (contact by stranger)	-2.406e-01	0.620832
condition (contract) by risk (texting and driving)	1.739e-01	0.731875
condition (software) by risk (texting and driving)	6.677e-02	0.890363
condition (contract) by risk (too much time online)	-5.217e-01	0.304020
condition (software) by risk (too much time online)	-8.012e-01	0.098145 .
condition (contract) by risk (viruses)	-1.739e-01	0.731875
condition (software) by risk (viruses)	-1.630e-01	0.736421
condition (contract) by evaluation (severity)	2.490e-01	0.632311
condition (software) by evaluation (severity)	4.652e-01	0.351692
condition (contract) by evaluation (child prevention)	4.875e-01	0.348845
condition (software) by evaluation (child prevention)	3.264e-01	0.511447
condition (contract) by evaluation (parent prevention)	1.170e+00	0.024596 *
condition (software) by evaluation (parent prevention)	6.857e-01	0.167820
participant (parent) by evaluation (severity)	-3.788e-01	0.025717 *
participant (parent) by evaluation (child prevention)	-4.234e-01	0.012494 *
participant (parent) by evaluation (parent prevention)	-4.363e-01	0.010237 *
condition (contract) by participant (parent)	5.678e-02	0.740399
condition (software) by participant (parent)	3.858e-01	0.017401 *
condition (contract) by risk (accidental adult content) by evaluation (severity)	-1.549e-01	0.829630
condition (software) by risk (accidental adult content) by evaluation (severity)	-5.720e-01	0.407170
condition (contract) by risk (accidental drug content) by evaluation (severity)	-4.783e-01	0.505249
condition (software) by risk (accidental drug content) by evaluation (severity)	-3.375e-01	0.623713
condition (contract) by risk (accidental self harm content) by evaluation (severity)	-5.649e-01	0.432671
condition (software) by risk (accidental self harm content) by evaluation (severity)	-3.476e-01	0.614466
condition (contract) by risk (online ads) by evaluation (severity)	-4.783e-01	0.505249
condition (software) by risk (online ads) by evaluation (severity)	2.696e-01	0.695163
condition (contract) by risk (being bullied) by evaluation (severity)	5.652e-01	0.431057
condition (software) by risk (being bullied) by evaluation (severity)	3.018e-01	0.660835
condition (contract) by risk (bullies another) by evaluation (severity)	-3.043e-01	0.671577
condition (software) by risk (bullies another) by evaluation (severity)	-2.770e-01	0.687211
condition (contract) by risk (illegal downloads) by evaluation (severity)	-1.348e+00	0.060472 .
condition (software) by risk (illegal downloads) by evaluation (severity)	-1.019e-01	0.882291
condition (contract) by risk (strained relationships) by evaluation (severity)	4.348e-02	0.951702
condition (software) by risk (strained relationships) by evaluation (severity)	2.754e-01	0.688872
condition (contract) by risk (poor schoolwork) by evaluation (severity)	-3.043e-01	0.671577

condition (software) by risk (poor schoolwork) by evaluation (severity)	-3.955e-01	0.564505
condition (contract) by risk (seeks adult content) by evaluation (severity)	-8.696e-02	0.903580
condition (software) by risk (seeks adult content) by evaluation (severity)	-2.339e-01	0.733839
condition (contract) by risk (seeks drug content) by evaluation (severity)	-3.478e-01	0.627993
condition (software) by risk (seeks drug content) by evaluation (severity)	-2.284e-01	0.739891
condition (contract) by risk (seeks self harm content) by evaluation (severity)	-8.696e-02	0.903580
condition (software) by risk (seeks self harm content) by evaluation (severity)	-1.763e-01	0.797757
condition (contract) by risk (too little sleep) by evaluation (severity)	5.797e-01	0.420679
condition (software) by risk (too little sleep) by evaluation (severity)	4.854e-01	0.481806
condition (contract) by risk (contact by stranger) by evaluation (severity)	-3.926e-01	0.585466
condition (software) by risk (contact by stranger) by evaluation (severity)	-7.672e-01	0.267254
condition (contract) by risk (texting and driving) by evaluation (severity)	-4.348e-01	0.544722
condition (software) by risk (texting and driving) by evaluation (severity)	-3.260e-01	0.635530
condition (contract) by risk (time) by evaluation (severity)	-1.739e-01	0.808564
condition (software) by risk (time) by evaluation (severity)	1.748e-01	0.799371
condition (contract) by risk (viruses) by evaluation (severity)	2.609e-01	0.716294
condition (software) by risk (viruses) by evaluation (severity)	1.808e-01	0.792726
condition (contract) by risk (accidental adult content) by evaluation (child prevention)	5.217e-01	0.467337
condition (software) by risk (accidental adult content) by evaluation (child prevention)	-6.211e-03	0.992766
condition (contract) by risk (accidental drug content) by evaluation (child prevention)	-8.696e-02	0.903580
condition (software) by risk (accidental drug content) by evaluation (child prevention)	1.025e-01	0.881075
condition (contract) by risk (accidental self harm content) by evaluation (child prevention)	-8.659e-02	0.904256
condition (software) by risk (accidental self harm content) by evaluation (child prevention)	4.103e-01	0.550459
condition (contract) by risk (online ads) by evaluation (child prevention)	-5.217e-01	0.467337
condition (software) by risk (online ads) by evaluation (child prevention)	2.345e-01	0.732140
condition (contract) by risk (being bullied) by evaluation (child prevention)	1.304e+00	0.069248 .
condition (software) by risk (being bullied) by evaluation (child prevention)	1.126e+00	0.100344
condition (contract) by risk (bullies another) by evaluation (child prevention)	3.478e-01	0.627993
condition (software) by risk (bullies another) by evaluation (child prevention)	4.798e-01	0.483668
condition (contract) by risk (illegal downloads) by evaluation (child prevention)	-4.348e-01	0.544722
condition (software) by risk (illegal downloads) by evaluation (child prevention)	4.457e-01	0.515338
condition (contract) by risk (strained relationships) by evaluation (child prevention)	3.043e-01	0.671577
condition (software) by risk (strained relationships) by evaluation (child prevention)	2.376e-01	0.728731
condition (contract) by risk (poor schoolwork) by evaluation (child prevention)	2.609e-01	0.716294
condition (software) by risk (poor schoolwork) by evaluation (child prevention)	7.065e-01	0.302388
condition (contract) by risk (seeks adult content) by evaluation (child prevention)	3.043e-01	0.671577
condition (software) by risk (seeks adult content) by evaluation (child prevention)	1.646e-01	0.810116
condition (contract) by risk (seeks drug content) by evaluation (child prevention)	1.304e-01	0.855811
condition (software) by risk (seeks drug content) by evaluation (child prevention)	6.537e-01	0.339949
condition (contract) by risk (seeks self harm content) by evaluation (child prevention)	3.478e-01	0.627993
condition (software) by risk (seeks self harm content) by evaluation (child prevention)	8.758e-01	0.201125
condition (contract) by risk (too little sleep) by evaluation (child prevention)	1.391e+00	0.052639 .
condition (software) by risk (too little sleep) by evaluation (child prevention)	1.447e+00	0.034673 *
condition (contract) by risk (contact by stranger) by evaluation (child prevention)	3.478e-01	0.627993
condition (software) by risk (contact by stranger) by evaluation (child prevention)	7.913e-02	0.908228
condition (contract) by risk (texting and driving) by evaluation (child prevention)	-2.609e-01	0.716294
condition (software) by risk (texting and driving) by evaluation (child prevention)	8.075e-02	0.906169
condition (contract) by risk (time) by evaluation (child prevention)	7.826e-01	0.275628

condition (software) by risk (time) by evaluation (child prevention)	7.593e-01	0.267697
condition (contract) by risk (viruses) by evaluation (child prevention)	7.391e-01	0.303182
condition (software) by risk (viruses) by evaluation (child prevention)	9.845e-01	0.150722
condition (contract) by risk (accidental adult content) by evaluation (parent prevention)	1.341e-13	1.000000
condition (software) by risk (accidental adult content) by evaluation (parent prevention)	-2.671e-01	0.696624
condition (contract) by risk (accidental drug content) by evaluation (parent prevention)	-2.621e-01	0.716614
condition (software) by risk (accidental drug content) by evaluation (parent prevention)	-5.716e-02	0.933938
condition (contract) by risk (accidental self harm content) by evaluation (parent prevention)	-6.518e-01	0.365248
condition (software) by risk (accidental self harm content) by evaluation (parent prevention)	-2.310e-01	0.736752
condition (contract) by risk (online ads) by evaluation (parent prevention)	-9.130e-01	0.203421
condition (software) by risk (online ads) by evaluation (parent prevention)	-1.071e-01	0.875712
condition (contract) by risk (being bullied) by evaluation (parent prevention)	9.130e-01	0.203421
condition (software) by risk (being bullied) by evaluation (parent prevention)	4.798e-01	0.483668
condition (contract) by risk (bullies another) by evaluation (parent prevention)	1.377e-13	1.000000
condition (software) by risk (bullies another) by evaluation (parent prevention)	-4.348e-02	0.949393
condition (contract) by risk (illegal downloads) by evaluation (parent prevention)	-9.565e-01	0.182723
condition (software) by risk (illegal downloads) by evaluation (parent prevention)	8.851e-02	0.897195
condition (contract) by risk (strained relationships) by evaluation (parent prevention)	6.004e-02	0.933531
condition (software) by risk (strained relationships) by evaluation (parent prevention)	1.485e-01	0.828853
condition (contract) by risk (poor schoolwork) by evaluation (parent prevention)	-3.043e-01	0.671577
condition (software) by risk (poor schoolwork) by evaluation (parent prevention)	-6.056e-02	0.929556
condition (contract) by risk (seeks adult content) by evaluation (parent prevention)	1.407e-13	1.000000
condition (software) by risk (seeks adult content) by evaluation (parent prevention)	-3.028e-01	0.658478
condition (contract) by risk (seeks drug content) by evaluation (parent prevention)	-3.913e-01	0.585671
condition (software) by risk (seeks drug content) by evaluation (parent prevention)	2.683e-01	0.695921
condition (contract) by risk (seeks self harm content) by evaluation (parent prevention)	4.348e-02	0.951702
condition (software) by risk (seeks self harm content) by evaluation (parent prevention)	2.174e-01	0.750981
condition (contract) by risk (too little sleep) by evaluation (parent prevention)	7.391e-01	0.303182
condition (software) by risk (too little sleep) by evaluation (parent prevention)	9.860e-01	0.150080
condition (contract) by risk (contact by stranger) by evaluation (parent prevention)	-2.609e-01	0.716294
condition (software) by risk (contact by stranger) by evaluation (parent prevention)	-4.348e-01	0.526447
condition (contract) by risk (texting and driving) by evaluation (parent prevention)	-6.087e-01	0.396467
condition (software) by risk (texting and driving) by evaluation (parent prevention)	-4.503e-01	0.510957
condition (contract) by risk (time) by evaluation (parent prevention)	6.462e-01	0.369384
condition (software) by risk (time) by evaluation (parent prevention)	8.543e-01	0.213840
condition (contract) by risk (viruses) by evaluation (parent prevention)	-2.609e-01	0.716294
condition (software) by risk (viruses) by evaluation (parent prevention)	-1.755e-01	0.797840
condition (contract) by participant (parent) by evaluation (severity)	3.885e-01	0.105288
condition (software) by participant (parent) by evaluation (severity)	-4.551e-01	0.047769 *
condition (contract) by participant (parent) by evaluation (child prevention)	-4.739e-01	0.047987 *
condition (software) by participant (parent) by evaluation (child prevention)	-9.635e-01	2.54e-05 ***
condition (contract) by participant (parent) by evaluation (parent prevention)	-7.190e-01	0.002736 **
condition (software) by participant (parent) by evaluation (parent prevention)	-9.611e-01	2.74e-05 ***

Signif. codes by 0 *** 0.001 ** 0.01 * 0.05 . 0.1   1

203

Table F.4: Model of survey participant exit data only, which examines primarily interactions between the factors of study condition, risk, participant age, and evaluation type.

Bibliography

[1] Child online protection act. `https://epic.org/free_speech/censorship/copa.html`, 1998.

[2] Children's online privacy protection rule ("COPPA"). `https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule`, 1998.

[3] Children's internet protection act. `https://www.fcc.gov/consumers/guides/childrens-internet-protection-act`, 2000.

[4] Kids & tech: The evolution of today's digital natives. Influence Central, `http://influence-central.com/kids-tech-the-evolution-of-todays-digital-natives/`, 2016.

[5] E. Aboujaoude, M. W. Savage, V. Starcevic, and W. O. Salame. Cyberbullying: Review of an old problem gone viral. *Journal of Adolescent Health*, 57(1):10–18, 2015.

[6] K. P. Allen. Off the radar and ubiquitous: Text messaging and its relationship to 'drama'and cyberbullying in an affluent, academically rigorous us high school. *Journal of Youth Studies*, 15(1):99–117, 2012.

[7] K. P. Allen. Tweeting, texting, and facebook postings: Stirring the pot with social media to make drama-case study and participant observation1. *The Qualitative Report*, 19(2):1, 2014.

[8] K. P. Allen. we dont have bullying, but we have drama: Understandings of bullying and related constructs within the social milieu of a us high school. *Journal of Human Behavior in the Social Environment*, 25(3):159–181, 2015.

[9] M. Anderson. Parents, teens and digital monitoring. *Washington, DC: Pew Internet & American Life Project. Retrieved January*, 9:2016, 2016.

[10] M. Anderson and J. Jiang. Teens, social media & technology 2018. *Washington, DC: Pew Internet & American Life Project. Retrieved June*, 3:2018, 2018.

[11] D.-. A. P. Association et al. Diagnostic and statistical manual of mental disorders. *Arlington: American Psychiatric Publishing*, 2013.

[12] R. Balebako, P. G. Leon, H. Almuhimedi, P. G. Kelley, J. Mugan, A. Acquisti, L. F. Cranor, and N. Sadeh. Nudging users towards privacy on mobile devices. In *Proc. CHI 2011 Workshop on Persuasion, Nudge, Influence and Coercion*, 2011.

[13] K. A. Bamberger and D. K. Mulligan. Privacy on the books and on the ground. *Stanford Law Review*, 63, January 2011.

[14] S. Bennett, K. Maton, and L. Kervin. The 'digital natives' debate: A critical review of the evidence. *British journal of educational technology*, 39(5):775–786, 2008.

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

[16] d. boyd. *It's Complicated: the social lives of networked teens.* Yale University Press, 2014.

[17] d. boyd, E. Hargittai, J. Schultz, and J. Palfrey. Why parents help their children lie to facebook about age: Unintended consequences of the childrens online privacy protection act. *First Monday*, 16(11), 2011.

[18] C. Bravo-Lillo, L. Cranor, S. Komanduri, S. Schechter, and M. Sleeper. Harder to ignore. *Revisiting pop-up fatigue and approaches to prevent it, USENIX Association*, pages 105–111, 2014.

[19] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, 9(2):18–26, 2011.

[20] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. Schechter. Your attention please: designing security-decision uis to make genuine risks harder to ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, page 6. ACM, 2013.

[21] A. Bruckman and A. Bandlow. The human-computer interaction handbook. chapter Human-computer Interaction for Kids, pages 428–440. L. Erlbaum Associates Inc., Hillsdale, NJ, USA, 2003.

[22] A. Bruckman, K. Luther, and C. Fiesler. When should we use real names in published accounts of internet research? *Digital Research Confidential: The Secrets of Studying Behavior Online*, page 243, 2015.

[23] M. Buhrmester, T. Kwang, and S. D. Gosling. Amazon's mechanical turk a new source of inexpensive, yet high-quality, data? *Perspectives on psychological science*, 6(1):3–5, 2011.

[24] J. K. Caird, K. A. Johnston, C. R. Willness, M. Asbridge, and P. Steel. A meta-analysis of the effects of texting on driving. *Accident Analysis & Prevention*, 71:311–318, 2014.

[25] M. Cecchinato, A. L. Cox, and J. Bird. "i check my emails on the toilet": Email practices and work-home boundary management. In *MobileHCI '14*, Toronto, Canada, September 2014. ACM.

[26] P. R. Center. Mobile fact sheet. `http://www.pewinternet.org/fact-sheet/mobile/`, January 2017.

[27] J. Cheng. What inner city kids know about social media, and why we should listen. Medium, September 25, 2013. `https://medium.com/i-m-h-o/53ea514c9ec0`.

[28] J. T. Child and D. A. Westermann. Let's be Facebook friends: Exploring parental Facebook friend requests from a communication privacymanagement (CPM) perspective. *Journal of Family Communication*, 13:46–59, 2013.

[29] L. F. Cranor, A. L. Durity, A. Marsh, and B. Ur. Parents' and teens' perspectives on privacy in a technology-filled world. In *Proc. SOUPS*, 2014.

[30] S. J. Czaja, W. A. Rogers, A. D. Fisk, N. Charness, and J. Sharit. *Designing for older adults: Principles and creative human factors approaches*. CRC press, 2009.

[31] A. Czeskis, I. Dermendjieva, H. Yapit, A. Borning, B. Friedman, B. Gill, and T. Kohno. Parenting from the pocket: Value tensions and technical directions for secure and private parent-teen mobile safety. In *Proc. SOUPS*, 2010.

[32] V. Della Cioppa, A. O'Neil, and W. Craig. Learning from traditional bullying interventions: A review of research on cyberbullying and best practice. *Aggression and Violent Behavior*, 23:61–68, 2015.

[33] J. S. Dumas, J. S. Dumas, and J. Redish. *A practical guide to usability testing*. Intellect books, 1999.

[34] S. Egelman and S. Schechter. The importance of being earnest [in security warnings]. In *International Conference on Financial Cryptography and Data Security*, pages 52–59. Springer, 2013.

[35] L. B. Erickson, P. Wisniewski, H. Xu, J. M. Carroll, M. B. Rosson, and D. F. Perkins. The boundaries between: Parental involvement in a teen's online world. *Journal of the Association for Information Science and Technology*, 2015.

[36] G. Feldman, J. Greeson, M. Renna, and K. Robbins-Monteith. Mindfulness predicts less texting while driving among young adults: Examining attention-and emotion-regulation motives as potential mediators. *Personality and individual differences*, 51(7):856–861, 2011.

[37] H. S. Ferdous, B. Ploderer, H. Davis, F. Vetere, K. O'Hara, G. Farr-Wharton, and R. Comber. TableTalk: Integrating personal devices and content for commensal experiences at the family dinner table. In *UbiComp '16*, Heidelberg, Germany, September 2016. ACM.

[38] R. Fleck, A. L. Cox, and R. A. Robison. Balancing boundaries: Using multiple devices to manage work-life balance. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 3985–3988. ACM, 2015.

[39] A. Forte, M. Dickard, R. Magee, and D. E. Agosto. What do teens ask their online social networks? social search practices among high school students. *CSCW*, 2014.

[40] K. France, A. Danesh, and S. Jirard. Informing aggression–prevention efforts by comparing perpetrators of brief vs. extended cyber aggression. *Computers in Human Behavior*, 29(6):2143–2149, 2013.

[41] W. O. Galitz. *The essential guide to user interface design: an introduction to GUI design principles and techniques*. John Wiley & Sons, 2007.

[42] M. Griffiths. Does internet and computer "addiction" exist? some case study evidence. *CyberPsychology and Behavior*, 3(2):211–218, 2000.

[43] L. Hale and S. Guan. Screen time and sleep among school-aged children and adolescents: a systematic literature review. *Sleep medicine reviews*, 21:50–58, 2015.

[44] L. Hanna, K. Risden, and K. Alexander. Guidelines for usability testing with children. *interactions*, 4(5):9–14, 1997.

[45] B. V. Hanrahan and M. A. Pérez-Quiñones. Lost in email: Pulling users down a path of interaction. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 3981–3984. ACM, 2015.

[46] S. T. Hawk, L. Keijsers, W. W. Hale III, and W. Meeus. Mind your own business! longitudinal relations between perceived privacy invasion and adolescent-parent conflict. *Journal of Family Psychology*, 23(4):511, 2009.

[47] C. Hax. Carolyn hax: Balancing trust and privacy when teens go online. https://www.washingtonpost.com/lifestyle/style/carolyn-hax-give-teenage-daughter-her-privacy-but-monitor-occasionally/2015/07/13/087083b0-201a-11e5-84d5-eb37ee8eaa61_story.html, July 2015.

[48] A. Hess. Millennials aren't oversharing on social media. (so what are they hiding?). Slate, October 18, 2013. http://www.slate.com/blogs/xx_factor/2013/10/18/millennials_on_social_media_young_people_are_incredibly_savvy_about_internet.html.

[49] D. Hill, N. Ameenuddin, Y. L. R. Chassiakos, C. Cross, J. Radesky, J. Hutchinson, A. Levine, R. Boyd, R. Mendelson, M. Moreno, et al. Media use in school-aged children and adolescents. *Pediatrics*, page e20162592, 2016.

[50] A. Hiniker, S. R. Hong, T. Kohno, and J. A. Kientz. Mytime: Designing and evaluating an intervention for smartphone non-use. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 4746–4757. ACM, 2016.

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

[52] C. D. Hunter. Social impacts: Internet filter effectiveness—testing over-and underinclusive blocking decisions of four popular web filters. *Social Science Computer Review*, 18(2):214–222, 2000.

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

[54] A. C. Johnston and M. Warkentin. Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, pages 549–566, 2010.

[55] A. Joyce. How to protect kids online: Apps and tactics used by experts—and real parents. https://www.washingtonpost.com/lifestyle/style/how-to-protect-kids-online-apps-and-tactics-used-by-experts--and-real-parents/2016/12/07/42ef7f14-ad13-11e6-a31b-4b6397e625d0_story.html, December 2016.

[56] S. P. Kiriakidis and A. Kavoura. Cyberbullying: A review of the literature on harassment through the internet and other electronic means. *Family & community health*, 33(2):82–93, 2010.

[57] S. G. Klauer, F. Guo, B. G. Simons-Morton, M. C. Ouimet, S. E. Lee, and T. A. Dingus. Distracted driving and risk of road crashes among novice and experienced drivers. *New England journal of medicine*, 370(1):54–59, 2014.

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

[59] M. Kwon, D.-J. Kim, H. Cho, and S. Yang. The smartphone addiction scale: development and validation of a short version for adolescents. *PloS one*, 8(12):e83558, 2013.

[60] M. Kwon, J.-Y. Lee, W.-Y. Won, J.-W. Park, J.-A. Min, C. Hahn, X. Gu, J.-H. Choi, and D.-J. Kim. Development and validation of a smartphone addiction scale (sas). *PloS one*, 8(2):e56936, 2013.

[61] C. Langos. Cyberbullying: The challenge to define. *Cyberpsychology, Behavior, and Social Networking*, 15(6):285–289, 2012.

[62] A. R. Lauricella, E. Wartella, and V. J. Rideout. Young children's screen time: The complex role of parent and child factors. *Journal of Applied Developmental Psychology*, 36:11–17, 2015.

[63] S.-J. Lee and Y.-G. Chae. Children's internet use in a family context: Influence on family relationships and parental mediation. *CyberPsychology & Behavior*, 10(5):640–644, 2007.

[64] A. Lenhart. Is the age at which kids get cell phones getting younger. *Pew Internet Research*, 2010.

[65] A. Lenhart, M. Duggan, A. Perrin, R. Stepler, H. Rainie, and K. Parker. Teens, social media & technology overview 2015. `http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/`, April 2015.

[66] K. E. Levay, J. Freese, and J. N. Druckman. The demographic and political composition of mechanical turk samples. *SAGE Open*, 6(1):2158244016636433, 2016.

[67] Y.-H. Lin, L.-R. Chang, Y.-H. Lee, H.-W. Tseng, T. B. Kuo, and S.-H. Chen. Development and validation of the smartphone addiction inventory (spai). *PloS one*, 9(6):e98312, 2014.

[68] R. T. Liu and B. Mustanski. Suicidal ideation and self-harm in lesbian, gay, bisexual, and transgender youth. *American journal of preventive medicine*, 42(3):221–228, 2012.

[69] S. Livingstone. Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New media & society*, 10(3):393–411, 2008.

[70] S. Livingstone. Online risk, harm and vulnerability: Reflections on the evidence base for child internet safety policy. *ZER: Journal of Communication Studies*, 18(35):13–28, 2013.

[71] S. Livingstone and M. Bober. Regulating the internet at home: contrasting the perspectives of children and parents. *Digital generations: Children, young people, and new media*, pages 93–113, 2006.

[72] S. Livingstone and L. Haddon. Risky experiences for children online: Charting european research on children and the internet. *Children & society*, 22(4):314–323, 2008.

[73] S. Livingstone, L. Haddon, A. Görzig, and K. Ólafsson. Risks and safety on the internet: the perspective of european children: full findings and policy implications from the eu kids online survey of 9-16 year olds and their parents in 25 countries. 2011.

[74] S. Livingstone and E. Helsper. Balancing opportunities and risks in teenagers use of the internet: The role of online skills and internet self-efficacy. *New media & society*, 12(2):309–329, 2010.

[75] S. Livingstone and P. K. Smith. Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of child psychology and psychiatry*, 55(6):635–654, 2014.

[76] M. Madden, S. Cortesi, U. Gasser, A. Lenhart, and M. Duggan. Parents, teens, and online privacy. Pew Internet Report, November 2012. `http://www.pewinternet.org/Reports/2012/Teens-and-Privacy.aspx`.

[77] M. Madden, A. Lenhart, S. Cortesi, U. Gasser, M. Duggan, A. Smith, and M. Beaton. Teens, social media, and privacy. Pew Internet Report, May 2013. `http://www.pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy.aspx`.

[78] A. Marsh, L. F. Cranor, and J. S. Downs. Experts' views on digital parenting strategies. Technical Report CMU-CyLab-17-002, Carnegie Mellon University, February 2017.

[79] A. Marwick and d. boyd. 'it's just drama': teen perspectives on conflict and aggression in a networked era. *Journal of Youth Studies*, 17(9):1187–1204, 2014.

[80] A. E. Marwick and d. boyd. Networked privacy: How teenagers negotiate context in social media. *new media & society*, page 1461444814543995, 2014.

[81] A. E. Marwick, D. M. Diaz, and J. Palfrey. Youth, privacy and reputation. *Harvard Law School Public Law & Legal Theory Working Paper Series*, pages 10–29, 2010.

[82] L. A. Matecki. Update: COPPA is ineffective legislation! Next steps for protecting youth privacy rights in the social networking era. *Northwestern Journal of Law & Social Policy*, 5(2):7:1–7:35, 2010.

[83] K. Mathiesen. The internet, children, and privacy: the case against parental monitoring. *Ethics and Information Technology*, 15(4):263–274, 2013.

[84] M. Mazmanian and S. Lanette. Okay, one more episode: An ethnography of parenting in the digital age. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, pages 2273–2286. ACM, 2017.

[85] A. Metzger, C. Ice, and L. Cottrell. But I trust my teen: Parents' attitudes and response to a parental monitoring intervention. *AIDS research and treatment*, 2012, 2012.

[86] K. J. Mitchell, D. Finkelhor, and J. Wolak. Protecting youth online: Family use of filtering and blocking software. *Child abuse & neglect*, 29(7):753–765, 2005.

[87] C. Moser, S. Y. Schoenebeck, and K. Reinecke. Technology at the table: Attitudes about mobile phone use at mealtimes. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 1881–1892. ACM, 2016.

[88] E. Nelson, P. Atchley, and T. D. Little. The effects of perception of risk and importance of answering and initiating a cellular phone call while driving. *Accident Analysis & Prevention*, 41(3):438–444, 2009.

[89] M. K. Nelson. *Parenting out of control: Anxious parents in uncertain times*. NYU Press, 2010.

[90] H. E. Nemme and K. M. White. Texting while driving: Psychosocial influences on young people's texting intentions and behaviour. *Accident Analysis & Prevention*, 42(4):1257–1265, 2010.

[91] B. C. Newell, C. A. Metoyer, and A. D. Moore. *Privacy in the Family*, pages 104–121. Cambridge University Press, 2015.

[92] J. Nielsen. *Designing web usability: The practice of simplicity*. New Riders Publishing, 1999.

[93] H. Nissenbaum. Privacy as contextual integrity. *Wash. L. Rev.*, 79:119, 2004.

[94] A. A. of Pediatrics. American Academy of Pediatrics announces new recommendations for children's media use. https://www.aap.org/en-us/about-the-aap/aap-press-room/pages/american-academy-of-pediatrics-announces-new-recommendations-for-childrens-media-use.aspx, October 2016.

[95] D. Olweus. Bullying at school. In *Aggressive behavior*, pages 97–130. Springer, 1994.

[96] D. Olweus. School bullying: Development and some important challenges. *Annual review of clinical psychology*, 9:751–780, 2013.

[97] J. W. Patchin and S. Hinduja. Measuring cyberbullying: Implications for research. *Aggression and Violent Behavior*, 23:69–74, 2015.

[98] G.-J. Y. Peters, R. A. Ruiter, and G. Kok. Threatening communication: a critical re-analysis and a revised meta-analytic test of fear appeal theory. *Health Psychology Review*, 7(sup1):S8–S31, 2013.

[99] S. Petronio. Privacy binds in family interactions: The case of parental privacy invasion. In W. R. Cupach and B. H. Spitzberg, editors, *The dark side of interpersonal communication*. Lawrence Erlbaum Associates, Inc, Hillsdale, NJ, 1994.

[100] M. Prensky. Digital natives, digital immigrants. *On the horizon*, 9(5):1–6, 2001.

[101] P. Resnick. Filtering information on the internet. *Scientific American*, 276(3):62–64, 1997.

[102] P. Resnick and J. Miller. Pics: Internet access controls without censorship. *Communications of the ACM*, 39(10):87–93, 1996.

[103] V. Rideout, C. Richardson, and P. Resnick. See no evil: How internet filters affect the search for online health information. 2002.

[104] J. A. Rode. Digital parenting: designing children's safety. In *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology*, pages 244–251. British Computer Society, 2009.

[105] F. Roesner, B. T. Gill, and T. Kohno. Sex, lies, or kittens? investigating the use of snapchat's self-destructing messages. In *International Conference on Financial Cryptography and Data Security*, pages 64–76. Springer, 2014.

[106] J. Rooksby, P. Asadzadeh, M. Rost, A. Morrison, and M. Chalmers. Personal tracking of screen time on digital devices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 284–296. ACM, 2016.

[107] L. D. Rosen, A. Lim, J. Felt, L. M. Carrier, N. A. Cheever, J. Lara-Ruiz, J. Mendoza, and J. Rokkum. Media and technology use predicts ill-being among children, preteens and teenagers independent of the negative health impacts of exercise and eating habits. *Computers in human behavior*, 35:364–375, 2014.

[108] J. Rubin and D. Chisnell. *Handbook of usability testing: how to plan, design and conduct effective tests.* John Wiley & Sons, 2008.

[109] A. J. Sedlak, D. Finkelhor, and J. M. Brick. National estimates of missing children: Updated findings from a survey of parents and other primary caretakers. *Juvenile Justice Bulletin. Washington, DC: US Department of Justice, Office of Justice Programs, Office of Juvenile Justice and Delinquency Prevention. NCJ*, 250089, 2017.

[110] V. M. Silenzio, P. R. Duberstein, W. Tang, N. Lu, X. Tu, and C. M. Homan. Connecting the invisible dots: Reaching lesbian, gay, and bisexual adolescents and young adults at risk for suicide through online social networks. *Social Science & Medicine*, 69(3):469–474, 2009.

[111] V. K. Singh, M. L. Radford, Q. Huang, and S. Furrer. " they basically like destroyed the school one day": On newer app features and cyberbullying in schools. In *CSCW*, pages 1210–1216, 2017.

[112] R. Slonje, P. K. Smith, and A. FriséN. The nature of cyberbullying, and strategies for prevention. *Computers in human behavior*, 29(1):26–32, 2013.

[113] J. G. Smetana. "It's 10 o'clock: Do you know where your children are?" Recent advances in understanding parental monitoring and adolescents' information management. *Child Development Perspectives*, 2(1):19–25, 2008.

[114] A. Smith. U.s. smartphone use in 2015. `http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/`, April 2015.

[115] D. J. Solove. Conceptualizing privacy. *California Law Review*, 90, 2002.

[116] D. J. Solove. "I've got nothing to hide" and other misunderstandings of privacy. *San Diego Law Review*, 44:745, 2007.

[117] D. J. Solove and P. M. Schwartz. *Privacy Law Fundamentals.* IAPP, 2013.

[118] A. Sternstein. Can parental spyware keep kids safe online? `http://www.csmonitor.com/World/Passcode/2017/0224/Can-parental-spyware-keep-kids-safe-online`, February 2017.

[119] How does teensafe work? `https://www.teensafe.com/blog/how-does-teensafe-work/`, January 2017.

[120] B. Teitell. In digital world, kids gain the upper hand. Boston Globe, September 5, 2013. `http://www.bostonglobe.com/lifestyle/style/2013/09/05/age-ubiquitous-screens-some-exhuasted-parents-have-stopped-policing`.

[121] B. Ur, J. Jung, and S. Schechter. Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 129–139. ACM, 2014.

[122] P. M. Valkenburg and J. Peter. Online communication among adolescents: An integrated model of its attraction, opportunities, and risks. *Journal of adolescent health*, 48(2):121–127, 2011.

[123] A. Vasalou, A.-M. Oostveen, and A. N. Joinson. A case study of non-adoption: the values of location tracking in the family. In *Proc. CSCW*, 2012.

[124] Y. Wang, P. G. Leon, A. Acquisti, L. F. Cranor, A. Forget, and N. Sadeh. A field trial of privacy nudges for facebook. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 2367–2376. ACM, 2014.

[125] Y. Wang, P. G. Leon, K. Scott, X. Chen, A. Acquisti, and L. F. Cranor. Privacy nudges for social media: an exploratory facebook study. In *Proceedings of the 22nd International Conference on World Wide Web*, pages 763–770. ACM, 2013.

[126] S. D. Warren and L. Brandeis. The right to privacy. *Harvard Law Review*, IV, December 1890.

[127] J. Weinberg. Rating the net. *Hastings Comm. & Ent. LJ*, 19:453, 1996.

[128] N. E. Willard. *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress*. Research Press, 2007.

[129] N. Wingfield. Should you spy on your kids? `https://www.nytimes.com/2016/11/10/style/family-digital-surveillance-tracking-smartphones.html`, November 2016.

[130] P. Wisniewski, A. K. Ghosh, M. Rosson, H. Xu, and J. M. Carroll. Parental control vs. teen self-regulation: Is there a middle ground for mobile online safety. In *Proceedings of the 20th ACM Conference on Computer Supported Cooperative Work & Social Computing, ACM*, 2017.

[131] P. Wisniewski, H. Jia, N. Wang, S. Zheng, H. Xu, M. B. Rosson, and J. M. Carroll. Resilience mitigates the negative effects of adolescent internet addiction and online risk exposure. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 4029–4038. ACM, 2015.

[132] P. Wisniewski, H. Jia, H. Xu, M. B. Rosson, and J. M. Carroll. Preventative vs. reactive: How parental mediation influences teens' social media privacy behaviors. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, pages 302–316. ACM, 2015.

[133] P. Wisniewski, H. Xu, M. B. Rosson, and J. M. Carroll. Parents just don't understand: Why teens don't talk to parents about their online risk experiences. In *Proceedings of the 2017 ACM Conference on Computer-Supported Cooperative Work & Social Computing*, 2017.

[134] P. Wisniewski, H. Xu, M. B. Rosson, D. F. Perkins, and J. M. Carroll. Dear diary: Teens reflect on their weekly online risk experiences. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 3919–3930. ACM, 2016.

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

[136] K. Witte. Fear as motivator, fear as inhibitor: Using the extended parallel process model to explain fear appeal successes and failures. *Communication Monographs*, 1998.

[137] J. Wolak, D. Finkelhor, and A. J. Sedlak. Child victims of stereotypical kidnappings known to law enforcement in 2011. *Juvenile Justice Bulletin*, pages 1–20, 2016.

[138] A. Woodruff, S. Augustin, and B. Foucault. Sabbath day home automation: it's like mixing technology and religion. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 527–536. ACM, 2007.

[139] S. Woolgar. Configuring the user: the case of usability trials. *The Sociological Review*, 38(S1):58–99, 1990.

[140] S. Yardi and A. Bruckman. Social and technical challenges in parenting teens' social media use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 3237–3246. ACM, 2011.

[141] M. L. Ybarra, D. Boyd, J. D. Korchmaros, and J. K. Oppenheim. Defining and measuring cyberbullying within the larger context of bullying victimization. *Journal of Adolescent Health*, 51(1):53–58, 2012.

[142] K. S. Young. Internet addiction: The emergence of a new clinical disorder. *CyberPsychology & Behavior*, 1(3):237–244, 1998.

[143] T. Zick. Congress, the internet, and the intractable pornography problem: The child online protection act of 1998. *Creighton L. Rev.*, 32:1147, 1998.

[144] I. Zych, R. Ortega-Ruiz, and R. Del Rey. Systematic review of theoretical studies on bullying and cyberbullying: Facts, knowledge, prevention, and intervention. *Aggression and Violent Behavior*, 23:1–21, 2015.