Circle of Trust: A New Approach to Mobile Online Safety for Families

Arup Kumar Ghosh
Department of Mathematical, Computing, and Information Sciences
Jacksonville State University
Jacksonville, AL, USA
akghosh@jsu.edu

Charles E. Hughes
Department of Computer Science
University of Central Florida
Orlando, FL, USA
ceh@cs.ucf.edu

Pamela J. Wisniewski
Department of Computer Science
University of Central Florida
Orlando, FL, USA
pamwis@ucf.edu

ABSTRACT

Traditional parental control applications designed to protect children and teens from online risks do so through parental restrictions and privacy-invasive monitoring. We propose a new approach to adolescent online safety that aims to strike a balance between a teen's privacy and their online safety through active communication and fostering trust between parents and children. We designed and developed an Android "app" called *Circle of Trust* and conducted a mixed methods user study of 17 parent-child pairs to understand their perceptions about the app. Using a within-subjects experimental design, we found that parents and children significantly preferred our new app design over existing parental control apps in terms of perceived usefulness, ease of use, and behavioral intent to use. By applying a lens of Value Sensitive Design to our interview data, we uncovered that parents and children who valued privacy, trust, freedom, and balance of power preferred our app over traditional apps. However, those who valued transparency and control preferred the status quo. Overall, we found that our app was better suited for teens than for younger children.

Author Keywords

Adolescent online safety; mobile smart phones; parental mediation; technical monitoring

CSS Concepts

• Human-centered computing > Human computer interaction (HCI) > Empirical studies in HCI

INTRODUCTION

Ninety-five percent of teens in the United States have access to a smartphone, and 45% of them are online 'almost constantly' [1]. Unfortunately, increased access to the internet through the unmediated use of smartphones exposes teens to a myriad of online risks. From watching inappropriate content, sexting, to chatting with strangers online, risks associated with smartphone use are becoming more commonplace for teens. For instance, 15% of teens say they send sexts, and 27% of teens have received them [51]. To keep their children safe from these online dangers, about 39% of parents report using parental control software for blocking, filtering or monitoring their teen's online activities on their home computers; yet, only 16% use parental controls on their teens' mobile smart devices [52]. This lower usage may be because recent research [7,15,33,40] has shown that parental control apps are overly restrictive, invasive of teens' personal privacy, and negatively impact teens' relationships with their parents. To try to overcome these problems, we conceptualized and implemented a new approach to mobile online safety by designing and developing *Circle of Trust*, an Android app for teens and their parents. Our approach aims to balance a teen's privacy with their parents' concerns for their online safety through fostering trust and communication between parents and children. We asked parent and children to share their opinions about *Circle of Trust,* based on the following research questions:

RQ1: *How does 'Circle of Trust' compare to traditional parental control apps?*

RQ2: *What are the different values in design that parents and children care about when making these comparisons?*

RQ3: *What specific features in 'Circle of Trust' do parents and children find useful (or not)?*

To answer these questions, we conducted a mixed methods user study with 17 parent-child (ages 9-17) pairs. Using a within-subjects experimental design, we found that parents and children significantly preferred our new app design over existing parental control apps in terms of perceived usefulness, ease of use, and behavioral intent to use. They also felt that *Circle of Trust* was significantly less privacy-invasive for children and would improve communication and the trust relationship between parent and child. Using the lens of Value Sensitive Design (VSD) [31], we also analyzed how participants felt about the apps based on family values that they mentioned during their interviews. Parents and children who preferred *Circle of Trust* tended to value the child's privacy, trust, freedom, and balancing the needs of

both parents and teens. Those who preferred the baseline parental control app put more value in transparency for the sake of safety and parental control. Through this research, we make the following unique research contributions:

- Designed and implemented an interactive artifact [70] in the form of an Android app called *Circle of Trust*.
- Compared *Circle of Trust* to the baseline features available in many commercially available parental control apps [66].
- Gained empirical (both quantitative and qualitative) insights from 17 parent-child pairs on the strengths and weaknesses of our new design.

In summary, we contribute a novel artifact developed through a theoretically validated approach to assess whether this artifact should be deployed longitudinally within families. The key contribution of this work is the care that was taken to minimize potential negative impacts [73] and ethically redesign existing parental control tools to better support parents and teens. Based on our findings, we provide actionable recommendations for iterating on the design of *Circle of Trust*, and more broadly, on designing adolescent online safety tools that support parents and teens.

BACKGROUND
In this section, we situate our research within the mobile online safety for adolescents literature and explain how our research leverages a Value Sensitive Design [30] approach.

Mobile Online Safety through Parental Control
Recently, the debate on whether mobile smartphones are harmful or helpful to teens has become a popular topic within the academic research community [22,39,46,74] and, more generally. within society as a whole [18,28,48]. Blackwell et al. [7] found that parents are often unaware about the types of social media apps their teens use and the frequency of use of these apps due to the limited visibility parents have into their teens' digital lives via their mobile devices. Gámez-Guadix et al. [32] found that teens are at least twice as likely to experience online sexual solicitations and have sex with a partner that they first met online when they have smartphones. This heightened risk perpetuates another point of controversy—whether and how parents should monitor their children's mobile smartphone and technology usage.

Those who have examined parental monitoring and parent-teen perceptions of risk (in offline contexts) have found that surveillance and tracking may not be the most effective solution, as it may perpetuate paranoia and fear on the part of both parents and teens [55,61]. For instance, Boesen et al. [8] examined mobile-based location tracking and found that such tracking devices had the potential to undermine trust. This has also been examined (with similar findings) by social computing researchers in at-home settings between family members [54,63]. A 2016 Pew Research study found that only 16% of parents use parental controls on teens' mobile smart devices to monitor their teens' mobile activities [52].Wisniewski et al. [66] shed some light as to why a

minority of parents choose to use parental control apps. In their analysis of 75 commercially available parental control apps, they found that most of the features supported parental control over teen-self regulation of their own behaviors. For instance, the apps gave parents granular access to monitor teens' intimate online interactions with others (e.g., every text message sent or received), and did very little to support teens as end users. Using the lens of Value Sensitive Design (VSD) [30], they argued that these apps do not reflect positive family values (e.g., trust, respect, empowerment) that should be encouraged within families.

Ghosh et al. [33] followed up by analyzing 736 Google Play reviews posted by children about these apps. They confirmed that teens strongly disliked parental control apps, finding them overly restrictive and privacy invasive to the point that the teens felt the apps harmed their relationship with their parents. Through a survey study of 215 parents and teens, Ghosh et al. [34] further confirmed that low autonomy-granting parents (e.g., authoritarian) were the most likely to use technical monitoring on their teens' mobile device, and teens who had parents who used parental control apps reported higher levels of online victimization and offline peer problems. This body of work [33,34,66,68] suggests that parental control apps may be detrimental to families, a teens' developmental growth, and the goal of keeping teens safe from online risks. Based on the limitations of existing parental control apps that were identified through this prior work, our aim was to conceptualize and design a new approach to mobile online safety that encompasses positive family values, as well as considers the needs of teens. Numerous researchers (e.g., [14,58,66,67,75]) have called for new sociotechnical solutions that move away from parental control toward promoting more teen-centric solutions. This research is a first step towards answering that call. In the next section, we introduce Value Sensitive Design [28] as the approach we used to create *Circle of Trust*.

A Theoretical Lens of Value Sensitive Design
Our study leverages VSD and builds upon Wisniewski et al.'s prior work [60] by conceptualizing, implementing, and evaluating a new mobile online safety app with the goal of promoting more positive family values through design. Value Sensitive Design (VSD) is "a theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process" [30]. VSD consists of conceptual, empirical, and technical investigations that help identify and embed human-values into the design of systems [31]. Past research on the topic of mobile online safety for teens has applied VSD principles to better understand the values and needs of parents and teens (c.f., [16,33,34,66]). For instance, Czeskis et al. [16] conducted semi-structured interviews of teens and their parents in order to understand the role of human values in mobile safety. In our study, we leveraged VSD in two ways: 1) in the iterative conceptualization and design of the features included in *Circle of Trust*, and 2) in the qualitative analysis for

identifying family values that influenced parents' and children's app preference during our user evaluation.

DESIGNING CIRCLE OF TRUST

In this section, we introduce Wisniewski et al.'s Teen Online Safety Strategies (TOSS) framework [66], which served as inspiration for the design of *Circle of Trust*. Then, we discuss the family values we incorporated in the design of our app.

The Teen Online Safety Strategies (TOSS) Framework

We drew from Wisniewski et al.'s TOSS framework as the grounding for designing *Circle of Trust*. The TOSS framework was theoretically derived to illustrate the tensions between parental control and teen self-regulation when it comes to teens' online behaviors, their desire for privacy, and their online safety [66]. In this framework, **parental control strategies** for online safety included: 1) *Monitoring:* passive surveillance of a teen's online activities [50], 2) *Restriction:* placing rules and limits on a teen's online activities, and 3) *Active Mediation:* discussions between parents and teens regarding their online activities [23,50]. In contrast, **teen self-regulation strategies** included: 1) *Self-Monitoring*, 2) *Impulse Control*, and 3) *Risk-Coping*. In order for teens to effectively self-regulate their online behaviors, they must be aware of their own actions through self-observation [3,45]. Impulse control aids in self-regulation by inhibiting one's short-term desires in favor of positive long-term consequences [6], and risk-coping is a component of self-regulation that occurs after one encounters a stressful situation, which involves addressing the problem in a way that mitigates harm [29,49]. Wisniewski et al.'s concluded that existing parental control apps implicitly valued parental authority and teen safety over teen privacy, trust, and open communication [66]. Thus, our goal was to develop an app that embedded these less emphasized values by design. We used the following design strategies to balance the value tensions of parents and teens:

Guidelines for Parental Control
- **Monitoring:** Preserve teen privacy through less granular activity monitoring risky activity.
- **Restriction:** Do <u>not</u> include features that restrict or control teens' online activities of behavior.
- **Active Mediation:** Prompt parents to engage with their teens to follow up on potentially risky online activities.

Guidelines for Teen Self-Regulation
- **Self-Monitoring:** Help raise the risk and self-awareness of teens by having them help monitor their own online activities.
- **Impulse Control:** Heighten self-awareness to help teens regulate their risk-related behaviors more intentionally.
- **Risk-Coping:** Aid in risk appraisals, so that teens can work with their parents to respond to potential threats.

Next, we describe the values we explicitly designed for when developing *Circle of Trust* based on these guiding principles.

Designing for Positive Family Values

We designed for the values of teen privacy, trust, and parental involvement. Below, we provide support from the literature as to why we chose to design for these values.

Designing for Teen Privacy

Privacy is a complex concept that has been theorized in numerous ways [2]. For instance, Petronio's Communication Privacy Management (CPM) theory [56], which is often applied within the context of families, frames privacy as an interpersonal boundary regulation process between parents and teens. This boundary is often marred with tension as parents and adolescents are in a constant push-pull process to negotiate between the teen's safety and well-being and their autonomy in online spaces [25]. Most research shows teens value their privacy, while interacting with others online [10,19,60,69]. Teen's need for privacy is directly tied to their need for autonomy and respect [57].

Designing for Trust

Trust is another important but equally complex concept, especially when mediated by technology. Harper *[36]* suggests that we should contextualize technology-mediated trust as "a continuation of the normal run of life" (p. 120) and focus on the kinds of "worry" that make us think about trust. In the case of families, trust is the critical factor in an adolescent's relationship with their parents *[65]*, where information disclosure from teens is necessary for "knowing" as a form of "trusting" *[43]*. Inversely, trust is tightly coupled with privacy for adolescents, where "trusting" is a form of giving a teen the space and autonomy to not disclose information *[57]*. Additionally, trust in the context of adolescent online safety involves the perceived (or real) safety (or danger) of others with whom a teen comes into contact and how this may disrupt the balance of privacy, trust, autonomy, and online safety within families *[25]*. Trust can be both a value (and a tension) used within the VSD process *[37,64]*. In a 2014 parent-teen interview study *[15]*, researchers reported that some degree of trust is needed to promote independence in teens. Prior trust between parent and teen improves the parent-teen relationship *[59]* and helps the child get involved in less high-risk behaviors *[9]*.

Designing for Parental Involvement

Responsiveness and demandingness are the two dimensions by which parenting styles vary. Responsiveness quantifies how much a parent is warm and supportive of their child's emotional and physical needs for autonomy [4,5]. Demandingness quantifies the behavioral and psychological control parents use in child rearing. Authoritative parents are both high on responsiveness and demandingness [21,26], and this type of highly involved parenting style is associated with positive youth outcomes that help children in their developmental growth [47]. Therefore, a shift towards more involved and supportive parent-child relationships has been advocated by researchers in the fields Human-Computer Interaction (HCI) and of adolescent online safety (c.f., [38,44,53,72,76]).

Translating Values into Design

The main features of *Circle of Trust* were mapped directly to the family values described above and the dimensions of the TOSS framework that were under-supported in Wisniewski et al.'s empirical app analysis as shown in **Table 1**. Our goal was to move away from parental control apps for online safety to more collaborative privacy-preserving apps that help parents and teens manage online risks together. Specifically, we moved away from parental control through privacy-invasive monitoring (mediated by trust-level) and restriction (which was completely removed as a design guideline) towards parental active mediation (parent dashboard), teen self-monitoring (teen dashboard), and risk-coping (risk flagging). For instance, we used risk-flagging, combined with metadata and trust-level to balance the trade-off between teen privacy and the parents' "need to know" that their teen was safe. We introduced a "Circle of Trust" feature by which parents and children could negotiate trusted and non-trusted contacts, and we designed the app for use jointly by parents and teens.

DESIGNING CIRCLE OF TRUST

Circle of Trust is a family online safety app that lets parents and children co-mediate the text messaging (i.e., SMS and MMS) activity that takes place via the child's phone. **Figure 1** illustrates the three main screens of *Circle of Trust*. In the sections below, we describe each of the main features. The novelty of our app comes from the use of summarization techniques (e.g., sentiment analysis, word cloud, risk-flagging) that share an abstraction of the child's online activities to their parents, rather than the actual message content. An additional unique characteristic of *Circle of Trust* is controlling this level of abstract through the trust by mutually negotiating safe and unsafe contacts.

Main Dashboard. The *Circle of Trust* dashboard is shown in **Figure 1(a)**. It provides a summary of all conversations the child had in the last two weeks prior to when the app was installed and thereafter. By default, all contacts are outside of the child's "Circle of Trust," indicated by the red shield

around the profile picture of the child's contacts. Contacts within the "Circle of Trust" are indicated by green shields. In the figure, two contacts are in the "Circle of Trust." The main dashboard also shows the number of messages sent/received and the number of risk alerts, which are indicated by the red triangle (in **Figure 1(a)**). Risk flags are explained in detail below.

Contact Summary. Upon clicking on a contact on the dashboard, the app provides a summary of the conversations, shown in **Figure 1(b)**. The contact summary page includes the following features, which are described in more detail below: (a) Circle of Trust, (b) Message Counts, (c) Risk Flags, (d) Sentiment Analysis, and (e) Image Word Cloud.

(a) *Circle of Trust Feature.* The idea of the "Circle of Trust" was inspired by research on healthy relationship formation and stranger safety for children with Autism [24]. The idea of trust circles was to help youth more accurately assess whether people they knew were safe or unsafe. We leveraged the concept to "trusted" and "untrusted" contacts in this first design iteration. At the top of the contact summary page, there is a switch for the "Circle of Trust" feature. By toggling this switch, the child can request that their parent add someone to their circle of trust. Similarly, from the parent's dashboard, the parent can add someone to their child's "circle of trust" or make a request that their child remove someone from the "circle of trust," who was previously approved by the parent. When the app is first installed, all contacts are outside of the circle of trust. After installation, parents and teens negotiate trust level of new contacts to jointly determine whether parents can view all text messages or only messages flagged with risks.

(b) *Message Counts.* This shows the number of messages exchanged between the child and a contact. The total is based on message content (i.e., texts, images, or videos) and the total for each type of message is shown as well.

(c) *Risk Flags.* The total number of flags is shown as well as the categorized totals by type (e.g., text, images, videos).

Design Justification	Circle of Trust Features						
	Main Dashboard	**Circle of Trust Feature**	**Message Counts**	**Risk Flags**	**Sentiment Analysis**	**Word Cloud**	**Message Details**
Values in Design							
Teen Privacy		X*	X	X*	X	X	X*
Trust		X		X			
Parental Involvement	X	X		X			
TOSS Framework							
Parental Monitoring	X	X	X	X	X	X	X
Restriction							
Active Mediation	X	X	X	X	X	X	X
Teen Self-Monitoring	X	X		X	X		
Impulse Control	X		X	X	X	X	
Risk-Coping	X	X		X	X	X	

Trust-level dictates level of privacy abstraction. When a contact is "trusted," parents only see risk-flagged content and message summaries using aggregation, sentiment analysis, and computer vision image object detection.

Table 1: Mapping Circle of Trust Features to TOSS Framework and Values in Design
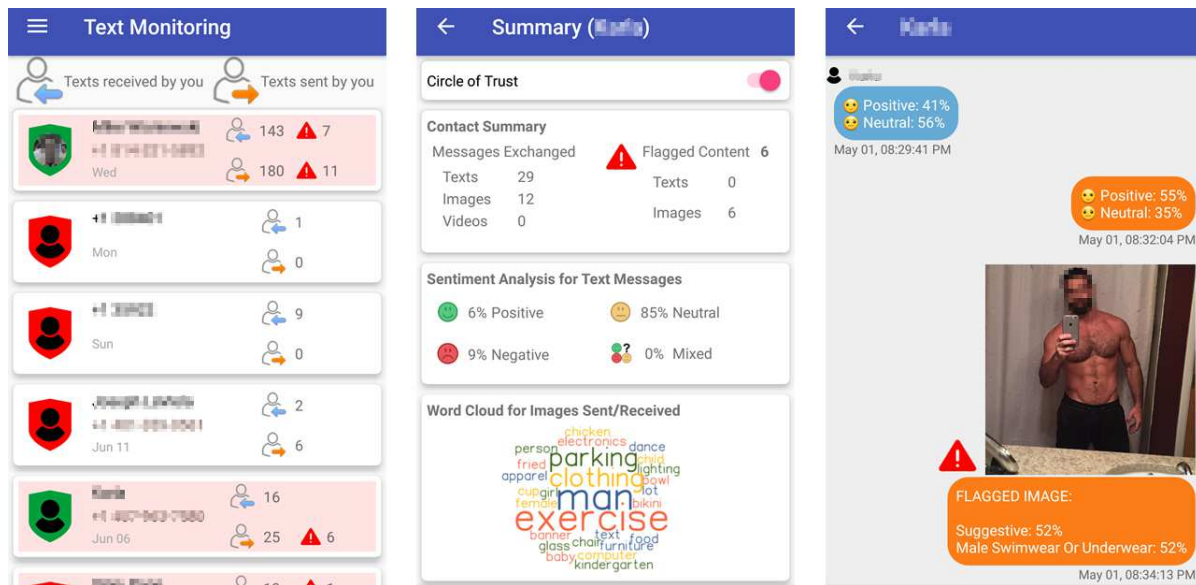
Figure 1: Circle of Trust App. (a) Teen Dashboard (b) Contact Summary (c) Message Details

Circle of Trust analyzes text messages and images for risk content using off-the-shelf risk detection APIs. Risk content includes profanity in text, and explicit/suggestive content in images. However, the app does not yet have the ability to analyze multimedia content other than images.

(d) ***Sentiment Analysis.*** The sentiment percentage score for each text is calculated, based on the extent to which a message is positive, negative, neutral, or mixed. An aggregated sentiment is shown for each conversation.

(e) ***Image Word Cloud.*** At the bottom of the contact summary screen, we used AWS's Rekognition API [77] to create a word cloud that visualized entities detected in images (not text) sent and received. A word cloud is an image composed of set of words, in which the size of each word indicates its frequency (e.g., more frequent, larger word). The intent was to give parents an idea of the types of images being exchanged while preserving the privacy of the actual photos. For example, in **Figure 1(b)**, the word cloud identified "man" and "exercise" as the prominent objects in the photo shown in **Figure 1(c)**.

Message Details. At the bottom of the contact summary screen, users can click on "Details" to view the message details for that contact as shown in **Figure 1(c)**. Based on trust level of a contact (i.e., trusted or untrusted), this feature varies the level of message details shared with the parent. For untrusted contacts, parents see all messages, like the baseline app. For trusted contacts, parents only see the actual message content for risk flagged content with an explanation of why it was flagged. Otherwise, the highest sentiment with percentage score for every text is shown. For flagged images, explicit/suggestive content percentage is shown along with the actual image.

System Implementation. The app architecture is based on the client-server model [78]. The server is an EC2 instance on Amazon Web Services. The server uses an encrypted connection for all communication with the clients. All server-side scripts were written in PHP. All data are stored securely on the server. Automated risk detection within SMS/MMS messages is performed using an API provided by a commercial parental control app and Amazon Comprehend [79] for text messages and Amazon Rekognition [77] for image processing, respectively.

METHODS

The primary goal of our study was to observe participants' initial reactions and identify potential pitfalls when using the app, so that we could redesign the app prior to conducting field studies. Below, we describe our study design. Then, we discuss the operationalization of our constructs, data analysis approach, recruitment of participants, and their profiles.

Study Overview

The user study consisted of two parts. 1) A within-group user study was run where each parent-child pair watched a video demo of (a) a baseline parental control app, and (b) *Circle of Trust*, They then interacted with both apps on phones provided by the researchers, and 2) A user study took place, where parent and children were asked to install *Circle of Trust* on their own mobile devices to perform a set of tasks. Participants were required to complete Part 1 prior to Part 2. Our rationale for having participants complete Part 1 prior to installing *Circle of Trust* on their own devices was to ensure that they had a full understanding of the nature of the app prior to consenting/assenting to take part in Part 2. Our goal was to mitigate the potential for violating the children's privacy and harming the parent-child relationship.

Part 1: A Baseline Comparison
To implement a within-subjects experimental design, we first developed a baseline app, so that participants had a comparison point for the status quo of parental control apps. We implemented a baseline comparison to reduce demand characteristics [20] and confirmation bias that participants liked "our" app. The baseline app was modeled after design patterns Wisniewski et al. [66] found to be included in most commercially available parental control apps. For instance, they found that most of these apps catered to parents, had limited interface features for teens, and "summary only monitoring was very uncommon, ranging between 0-3% of all apps" [66]. When text message monitoring was available, parents were given low-level message details; thus, the baseline app was designed per their findings: 1) the baseline app sends parents the content of every text message the child sends or receives, 2) the app has a user interface for the parent, but there is no user interface for the child, and 3) the app sends the unfiltered text messages to the parent.

Participants completed the IRB approved consent/assent form and took a pre-survey. Next, they watched a video demo of either the baseline app or *Circle of Trust* and explored the apps on a phone provided by the researchers. To avoid ordering effects, the study was counter-balanced by alternating which app was presented first to each new participant pair who enrolled in the study. Next, we administered a post-survey, and the same process was repeated for the second app. The study concluded with a short, semi-structured interview, which we video- or audio-recorded based on participants' choice. Part 1 of the study took about one hour to complete. Each participant received a $10 Amazon gift card (totaling $20 for the pair).

Research Hypotheses
We proposed the following hypotheses for Part 1:

H1: *Parents and children will prefer Circle of Trust over the baseline app in terms of: (a) Perceived Usefulness, (b) Ease of Use, and (c) Behavioral Intent to Use.*

H2: *Parents and children will prefer Circle of Trust over the baseline app in terms of: (a) Online Risk Mediation, (b) Privacy Invasiveness, (c) Active Mediation, (d) Self-Monitoring, and (e) Relational Trust- Harm.*

Next, we describe how we operationalized these measures.

Operationalization of Constructs
Post-surveys were used to capture dependent measures and to test our research hypotheses. Pre-validated dependent measures included technology acceptance model variables [17], including usefulness, ease of use, and behavioral intent to adopt. We used the technology acceptance measures as a proxy for assessing whether *Circle of Trust* would be a better alternative than the baseline app. We created new constructs for evaluating TOSS related outcomes as shown in **Appendix Table 3** added as a supplementary document. We also created new constructs to measure online risk mediation, privacy invasiveness, and relational trust-harm. The privacy

invasiveness measure was created based on prior qualitative work with parents and teens regarding privacy boundary turbulence [15,25]. We evaluated the construct validity for each measure using Cronbach's alpha, and all were above the 0.7 threshold for acceptability (as shown in **Table 2**). In the pre-survey, we also collected demographic information about our participants, as well as contextual information, including the Parenting Style Index [62]. In the following section, we describe Part 2 of our user study.

Part 2: Using Circle of Trust to Perform a Guided Task
In Part 2, participants were asked to install *Circle of Trust* on their own Android mobile devices. Once both parent and child installed the app, they were asked to complete pre-defined tasks using the app. These tasks included deciding which contacts should be added to the child's trust circle and reviewing risk flags together. We asked participants to think aloud [35] during this exercise. After completing the task, we concluded the study with a brief exit interview. The session was video- or audio-recorded and transcribed. We also took high-level observational notes on how parents and children interacted with one another and the app. Participants also completed a survey assessing each of the main features of *Circle of Trust* after they completed the tasks. All features were rated on a 5-point Likert scale from "extremely bad" to "extremely good." Part 2 of our study took approximately 2 hours and once it was complete, we helped the participants uninstall the app and each parent and child received an additional $15 dollars Amazon gift card for their time (totaling $30 for the pair).

Data Analysis Approach
We conducted a mixed-methods, quantitative and qualitative analyses of our data to: 1) empirically test our research hypotheses and 2) gain additional insights from parents and children as to their perceptions about the two apps. For the within-subject design for Part 1, we used IBM SPSS Statistics 24 [80] to conduct paired t-tests or Wilcoxon signed-rank tests based on normality results to determine if there were significant effects of our treatment (i.e. baseline app versus *Circle of Trust*) on the dependent constructs. We used the Shapiro-Wilk Test for determining normality, also shown in the table; if the p-value was below 0.05, the data deviated significantly from a normal distribution. If this were the case, we used the appropriate non-parametric test to assess the statistical difference.

For our qualitative analysis, we conducted a standard content analysis [12], where one counts the frequency of concepts that occur across transcripts. We used the lens of value-sensitive design to identify the emergent values, then we assessed how these values were used as a rationale for preferring one app over the other. We analyzed the think aloud transcripts for value-based evaluations of the app, which were included in our qualitative results. The first author coded transcripts and iteratively recoded the data based on daily feedback from the last author. Through this process, we gained valuable insights on what values parents

and children thought were important in the context of designing family safety systems and how these values were associated with *Circle of Trust* and the baseline app. Parents and children discussed multiple values that led them to prefer one app or another, and at times, changed their preference based on the value they were discussing at the time. Therefore, we report our findings based on their values and which values aligned with their app preferences.

Participant Recruitment and Profiles

We recruited children ages 9 through 17 years of age (teens and younger children will collectively be referred to as "children" from this point forward). Prior research [33] shows that children start using smartphones prior to adolescence, some as young as nine years-old. Therefore, we expanded the age range of participants from teens (13-17) to include younger children (9-12) who use smartphones. Teens and younger children will collectively be referred to as "children" from this point forward. This gave us an opportunity to assess whether our app would be well-suited for younger children. To participate in the study, each child was required to use SMS/MMS text messaging on their phones and have a parent or legal guardian of at least 18 years of age participant in the study with them. Recruitment was done by word-of-mouth and by contacting more than 20 youth serving organizations. We also sent recruitment e-mails to our department's mailing list and distributed a flyer to local community groups. Most of our participants were recruited from public libraries, YMCAs, and an Indian community group. A power analysis using G*Power [27] determined that with a matched pairs, within dependent means t-test for a large effect size (Cohen's d = 0.8, α=0.05,

and Power = 80%), a sample size of 15 was needed to test our Part 1 hypotheses. We recruited 17 parent-child pairs for Part 1, and eight pairs continued to Part 2. The participants who did not complete Part 2 often made this choice due to time constraints not having an Android device. Data collection ended in May 2018.

Children were 9-17 years old with average age 13.5 years. Parents were mostly between ages 31-40 (8) and 41-50 years (8), except one who was older. Most of the children were female (9) and most parents (10) were male. Children identified themselves as Asian (8), Hispanic/Latino (3), Black/African American (1), and other ethnic origins. Parents reported similar ethnic backgrounds. Nine parents indicated that they had a Master's degree. Other parents had either a four-year (7) or a two-year (1) college degree. The annual household income varied from under $30k (1), $30-$60k (3), $80k-$100k (1), $100k-$150k (8), and over $150k (3). Five parents reported using parental control apps on their child's mobile device (e.g., Screen Time, Google a/c, Zift, T-mobile, Microsoft, and OurPact), and four of the children were aware they were being monitored. All four parenting styles were represented across our sample: authoritative (6), authoritarian (6), neglectful (4), and permissive (1).

RESULTS

Hypotheses Testing Results (RQ1)

Table 2 includes mean, median, and standard deviation for all the dependent measures for children (C) and parents (P). Bolded rows indicate the difference test was statistically significant. For the most part, parents and children significantly preferred *Circle of Trust*. Parents and children

Measure (Cronbach's ∝)	C/P	Normality Test^		Mean		Median		St. Dev.		Diff. Test^^
		TXT	COT	TXT	COT	TXT	COT	TXT	COT	
Usefulness (0.93)	C	**0.95**	**0.88***	**4.20**	**5.34**	**3.83**	**5.5**	**1.47**	**0.98**	**-2.37***
	P	**0.89***	**0.95**	**4.44**	**5.40**	**4.5**	**5.67**	**1.36**	**0.84**	**-2.31***
Ease of Use (0.95)	C	**0.91**	**0.95**	**5.26**	**6.09**	**5.33**	**6.0**	**1.16**	**0.63**	**-2.64***
	P	0.88*	0.73***	5.92	6.05	6.17	6.5	0.99	1.24	-0.74
Intent to Use (0.97)	C	**0.90**	**0.96**	**2.33**	**3.24**	**2.0**	**3.0**	**0.76**	**0.99**	**-3.39****
	P	**0.92**	**0.8***	**3.20**	**4.04**	**3.0**	**4.0**	**1.24**	**1.18**	**-2.33***
Risk Mediation (0.92)	C	0.81**	0.88*	3.93	4.43	4.5	4.5	1.16	0.54	-1.07
	P	0.81**	0.7***	4.04	4.54	4.5	5.0	1.12	0.70	-1.26
Privacy Invasiveness (0.83)	C	**0.94**	**0.90**	**3.65**	**2.45**	**3.67**	**2.33**	**1.03**	**0.54**	**4.86****
	P	**0.87***	**0.93**	**3.82**	**2.52**	**4.0**	**2.67**	**0.72**	**0.79**	**-3.33****
Active Mediation (0.72)	C	0.89*	0.96	3.63	3.84	3.67	4.0	0.76	0.71	-1.17
	P	**0.91**	**0.87***	**3.67**	**4.22**	**4.0**	**4.0**	**0.71**	**0.51**	**-2.13***
Teen Self-Monitoring (0.90)	C	0.96	0.89*	3.33	3.96	3.33	4.0	1.14	0.47	-1.89
	P	0.85*	0.82**	4.1	4.47	4.0	4.67	0.80	0.49	-1.32
Relational Trust-Harm (0.70)	C	**0.91**	**0.94**	**3.25**	**2.55**	**3.67**	**2.33**	**1.0**	**0.74**	**3.22****
	P	**0.91**	**0.94**	**3.24**	**2.61**	**3.33**	**2.33**	**0.7**	**0.77**	**2.65***

∝ = *Cronbach's* ∝; *C=Child; P=Parent; TXT=Text Messaging Parental Control App; COT=Circle of Trust;* ^ *Shapiro-Wilk Test was used for determining normality, if p-value is below 0.05, the data deviate significantly from a normal distribution;* ^^*Median and Wilcoxon Signed Ranked tests were used for assessing non-normal data;* * *Denotes p-value <= 0.05,* ** *<= 0.01,* *** *<= 0.001*

Table 2: Reliability Metrics and Descriptive Statistics for Dependent Measures

preferred *Circle of Trust* over the baseline app in terms of: Usefulness (**H1a**), Behavioral Intent to Use (**H1c**), Privacy Invasiveness (**H2b**), Relational Trust-Harm (**H2e**). Children preferred *Circle of Trust* over the baseline app in terms of Ease of Use (**H1b**) and parents preferred *Circle of Trust* over the baseline app in terms of: Active Mediation (**H2c**). We did not find any significant results for: Risk Mediation (**H2a**) and Teen Self-Monitoring (**H2d**). Also, Ease of Use (H1b) for parents and Active Mediation (**H2c**) for children were not supported. We also tested for paired differences between parents and children for all the dependent measures. Parents reported significantly higher child self-awareness for *Circle of Trust* than children (Z=-2.923, p=0.003). Parents' behavioral intent to use of the baseline app was significantly higher than those of children (t(16)=-3.080, p<=0.01). No other statistically significant differences were found between parents and their children.

The Values that Mattered within Families (RQ2)
In this section, we present the most frequently discussed values in relation to what participants thought about the two apps. Respecting a child's privacy was the most frequently mentioned value (N=31 out of 34 participants), followed by promoting parent-child trust (N=18), facilitating open communication (N=14), and negotiating control between parents and children (N=14). In most cases, these values led participants to prefer the design of *Circle of Trust* over the baseline parental control app. In the sections below, we describe each value and how this value played a role in how children and parents evaluated the apps.

Respecting the Privacy of the Child
Most children (13 out of 17) preferred *Circle of Trust* because it gave them more privacy. Parents only saw risk-flagged content for trusted contacts, which made children feel better about their parents monitoring their text messages:

"Your parents can not see everything. Not that I can get away with things. It [Circle of Trust] shows less and it shows bad things- not the exact word." –C1, 14-year old male

Many children explained that they would be uncomfortable texting if they had no privacy from their parents, indicating they would even use a different messaging platform, if the baseline app were installed on their phones:

"I feel like you are not giving your child and her friend privacy. ... I will not feel comfortable texting with my friends about what we talk about." –C2, 16-year old female

Similarly, most parents (13 out of 17) valued their children's privacy and preferred *Circle of Trust*. They thought that this app was less privacy-invasive than the baseline app, which they thought would invade their child's privacy:

"In the first app [baseline app], it looks like I am invading her privacy a lot. I was getting to know things I might not want to. But here [Circle of Trust] she gets her privacy."– P8, Mother of 15-year old female

On the other hand, some parents of younger children thought that, at their children's age, privacy was not important. According to them, their children were not mature enough to differentiate between right and wrong by themselves.

"Privacy is not important at this age ... at her age, she does not know, what is good, what is bad."–P9, Mother of 10-year old female

Overall, most children and parents wanted their child to have some level of privacy, and hence, preferred *Circle of Trust* over the baseline app for this reason.

Promoting Trust between Parent and Child
Some children (6 out of 17) thought that using *Circle of Trust* would improve their trust relationship with parents. According to them, using the baseline app would question the existence of trust between parent and child:

"If you are using [Circle of Trust] then your child realizes that my parents trust me at certain level and if you are using text messaging [baseline] app and see all messages then your child thinks my parent don't trust me, they think I might do something wrong."–C15, 15-year old male

However. some younger children preferred the baseline app as it would allow their parents to teach them how to safely interact with others and build trust. Yet, when they grew older, they would value being able to confide in their friends without their parents' supervision:

"May be for children baseline app would be better. So that child can discuss with their parents what did they did wrong and how he can they improve in texting. But when they grow older ... Circle of Trust would be better ... Based on if they are trusted or not, child can confess their own thoughts with their friends." –C12, 10-year old female

Over half of the parents (9 out of 17) agreed that trusting their children was necessary as they grow older. Otherwise, a lack of trust would hurt the relationship with their children:

"When you are bringing up your child you need to trust them at a certain point of time ... Unless you trust them to a certain level, it's very difficult to maintain certain sort of relationship with them. So, I feel the first app [Circle of Trust] is better."–P5, Mother of 12-year old female

In summary, parents and children believed that *Circle of Trust* would help them build parent-child trust. A lack of trust might hurt parent-child relationships, especially as children matured into teens. Younger children and their parents would like to use the baseline app more, but these parents would consider increasing trust over time.

Facilitating Open Communication
Some children (4 out of 17) thought that *Circle of Trust* would help them communicate better with their parents. When a child was too scared or uncomfortable to approach their parent for help, they felt that the app could help initiate those types of hard conversations:

"... the kid does not have to be the one going and asking for help. The parents can go and like 'hey you know I see that's happening' and confront the kid about it instead of the kid having to confront them. Because if they [children] are insecure then confrontation is not the thing they want to do at all."–C17, 17-year old female

Over half of the parents (9 out of 17) also liked how *Circle of Trust* helped them teach their children whom they should and should not trust. The *Circle of Trust* app would facilitate more communication as part of this negotiation process:

"And we can discuss why they are not [trusted]. What is inappropriate about it and why certain friends are [trusted]. Communication would increase between me and my child." –P1, Father of 14-year old male

Parents and children generally liked the communication between parent and child and preferred to use *Circle of Trust*. They felt that communication would help children learn more about online safety and would promote positive parent-child relationship. However, one parent preferred open communication with his child to the extent that he preferred not to use any app at all. Yet, he said that if he had to use an app, then *Circle of Trust* would be much better for his family.

Negotiating Control between Parents and Children
Some children (5 of 17) liked *Circle of Trust* as it would give them some control to decide who should be in their trust circle, and who should be outside of it:

"I like the Circle of Trust app probably because it allows me as the child [to] decide who you do want in your circle and who you do not want in your circle."–C2, 16-year old male

Similarly, some parents (5 out of 17) liked the fact that *Circle of Trust* gave children and parents the ability to negotiate which contacts would be trusted or not. The ability to negotiate boundaries through the app was helpful. These parents liked the fact that in *Circle of Trust* presented the interaction as a request of the child instead of a demand:

"Because, it never kind of forcing you to...I am requesting."– P14, Father of 11-year old male

Parents generally liked the idea of having more control than their children when making decisions. Some parents of younger children did not want to give their child more freedom. However, they were open to giving their child more freedom as they got older:

"You can differentiate based on ages…the age may be from 9-10 years to say 14-15 years maybe it's better to use the second one [baseline app]. I think when they cross 15, then I think the first [Circle of Trust] will be beneficial. Because then they are more aware of the society, they are more aware of themselves." –P12, Father of 10-year old female

App preference based on age was a common theme we found when it came to negotiating control. Parents and children mentioned other values during the interviews, including the importance of safety, the convenience of using risk-flagging
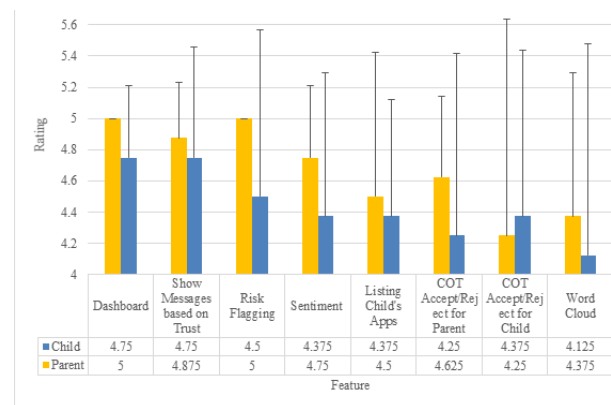

Figure 2: Parent-Child Evaluations of Circle of Trust Features

to assist with monitoring, teaching good decision making, and helping children be more aware of their own actions. However, these values did not emerge as frequently.

A Feature-based Assessment of Circle of Trust (RQ3)
In the post-survey for Part 2, we asked parents and children (N=8 pairs) to rate the features of *Circle of Trust*. **Figure 2** shows mean ratings for the main features of *Circle of Trust* with bars indicating standard deviations. We ordered the features by the cumulative average of parents and children in descending order. The "Dashboard" was the most popular feature among participants, and "Word Cloud" was the least popular feature. Children particularly liked having access to their own dashboard. Overall, parent ratings were higher than those from children, except for the "Circle of Trust Accept/Reject for Child" feature, where children had to approve if the parent wanted to remove a trusted contact from their "Circle of Trust." Children rated this feature more favorably than parents. Parents were ambivalent about negotiating with their children about which contacts should be in the child's trust circle. Some parents were against their child having accept/reject decision power, acknowledging that it would be difficult to give up that level of control:

"The feature I didn't like is obviously the accept/reject feature for child because as a parent you wanna be more in control of that feature than allowing them to have control of that. So it's kind of reverse of what she was saying [smiling]."–P2, Father of 16-years old female

Overall, the results from Part 2 reconfirmed many of the value-based themes from Part 1 of our study. Yet, we gained insight into features that needed to be iterated upon in our next version of *Circle of Trust*.

DISCUSSION
Below, we discuss the implications of our results, the limitations of our work, and future research directions.

Differentiating between Children and Teens
A benefit (and lesson-learned) from our choice to include younger children in our study was that it confirmed our earlier assumption that online safety apps should be uniquely

designed for different age groups. Overall, our findings suggest that *Circle of Trust* is more appropriate for teens as opposed to younger children. This presents an interesting research question for how one might transition the app from giving higher levels of parental control for younger children to more personal agency to self-regulate once children become teens. This is a challenge that commercial entities, such as Google's Family Link, have also had to address [13] within their platforms, as 13 is the legal age of consent on the internet. One potential way to do this would be to incorporate customizable features targeted towards shifting the balance between increased parental control or teen autonomy. The app might suggest certain features based on the child's age and nudge parents to adjust these features over time. Otherwise, a teen could request a certain feature be turned on or off based on earning trust from their parents. Making family monitoring apps developmentally appropriate based on the age of the child is a worthy area of further exploration.

Reflecting on When Trust Begins

Participants raised concerns about contacts being out of the "Circle of Trust" right after installing the app, and parents being able to read all the child's messages sent/received in the last 14 days. This concern raised a basic question about the starting point of parent-teen trust. Should we, by default, assume no trust and then work up to trusting people? Or should we, by default, assume everybody is trusted and then they fall out of trust if there is a risk flag? As a parent suggested during our study, we plan to redesign the app to bring up the contact list first and have parents and teens work together to decide who belongs in the trust circle before message details are shown to parents. Alternatively, during the installation of the app, we could ask parent and child what trust circle model (i.e., trusted/non-trusted or spectrum of trust) they would like to use to perform the initial negotiation on trust circle membership (they could choose between showing the contact list first or showing the actual conversations). Otherwise, we might have a spectrum of trust or multiple circles of trust. Implementing a layered "Circles of Trust" that can adjust more intelligently to notify parents when they need to pay immediate attention to a situation is another avenue we plan to explore.

Moving towards Teen Self-Regulation

Circle of Trust did not support risk mediation or child self-monitoring any better than the baseline app (**Table 2**). This suggests that the app, in its present form, lacks features that could help teens self-regulate their online behaviors and assess the quality of their relationship with their friends. What feature could help teens be more reflective about their relationships? We could potentially implement a feature that leverages validated approaches to help teen assess friendship quality [11] for all their contacts. However, more work needs to be done to understand how best to support teen self-regulation and to teach them how to be good digital citizens [42]. Thus, we plan to conduct participatory design sessions with teens to improve these capabilities prior to launching a longitudinal field study.

Limitations and Future Research

We counter-balanced the sessions to minimize potential ordering effects and presented the same evaluative questions to participants for each app, both of which we designed and built, so that they would be consistent in terms of look and feel. However, demand characteristics (participants trying to please researchers [20]) may still have influenced our results. Between group user studies or field studies should be done to further reduce bias. Another potential bias is that eight parent-teen pairs were recruited from an Indian community group. Indian mothers in America are more likely to use authoritative parenting styles, while parents residing in India are more inclined to use authoritarian parenting styles [41]. The Indian parents in our sample were a mixture of parenting styles: authoritative (2), authoritarian (2), neglectful (3), and permissive (1), and we received a wide range of perspectives from these families. Therefore, we do not believe that sampling from this population biased our results. On the contrary, we believe that drawing participants from non-white families is a contribution of this work. Similar to Yardi et al. [71], future studies should continue to diversify their sampling procedures to include families of color. Overall, our results are generalizable to the extent that they show that the values we intended to embed in *Circle of Trust* were mostly translated into design. More importantly, our empirical study pinpointed key opportunities for redesign. Based on our findings, we will iterate on *Circle of Trust* prior to conducting longitudinal field studies with families.

CONCLUSION

We conceptualized a new approach to adolescent mobile online safety, developed an Android app called *Circle of Trust,* and explored this app in comparison to the status quo of parental control apps. Participants found our Value-Sensitive Design approach less privacy-invasive for teens and beneficial to the parent-child trust relationship. We provided implications of our results and then suggested designs that would help create effective mobile online safety solutions and promote positive parent-teen relationships.

ACKNOWLEDGMENTS

REFERENCES

[1]   Monica Anderson and Jingjing Jiang. 2018. Teens, Social Media & Technology 2018. *Pew Research Center: Internet, Science & Tech*. Retrieved September 10, 2018 from http://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018/

[2]   Karla Badillo-Urquiola, Yaxing Yao, Oshrat Ayalon, Bart Knijnenurg, Xinru Page, Eran Toch, Yang Wang, and Pamela J. Wisniewski. 2018. Privacy in Context: Critically Engaging with Theory to Guide

Privacy Research and Design. In *Companion of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing* (CSCW '18), 425–431. https://doi.org/10.1145/3272973.3273012

[3]   Albert Bandura. 1991. Social Cognitive Theory of Self-Regulation. *Organizational Behavior and Human Decision Processes* 50, 2: 248–287. https://doi.org/10.1016/0749-5978(91)90022-L

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

[5]   Diana Baumrind. 2005. Patterns of parental authority and adolescent autonomy. *New Directions for Child and Adolescent Development* 2005, 108: 61–69. https://doi.org/10.1002/cd.128

[6]   Antoine Bechara. 2005. Decision making, impulse control and loss of willpower to resist drugs: a neurocognitive perspective. *Nature Neuroscience* 8, 11: 1458–1463. https://doi.org/10.1038/nn1584

[7]   Lindsay Blackwell, Emma Gardiner, and Sarita Schoenebeck. 2016. Managing Expectations: Technology Tensions Among Parents and Teens. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (CSCW '16), 1390–1401.

[8]   Julie Boesen, Jennifer A. Rode, and Clara Mancini. 2010. The Domestic Panopticon: Location Tracking in Families. In *Proceedings of the 12th ACM International Conference on Ubiquitous Computing*, 65–74.

[9]   Elaine A. Borawski, Carolyn E. Ievers-Landis, Loren D. Lovegreen, and Erika S. Trapl. 2003. Parental monitoring, negotiated unsupervised time, and parental trust: the role of perceived parenting practices in adolescent health risk behaviors. *The Journal of Adolescent Health: Official Publication of the Society for Adolescent Medicine* 33, 2: 60–70.

[10] danah boyd. 2014. *It's Complicated: The Social Lives of Networked Teens*. Yale University Press, New Haven.

[11] William M. Bukowski, Betsy Hoza, and Michel Boivin. 1994. Measuring Friendship Quality During Pre- and Early Adolescence: The Development and Psychometric Properties of the Friendship Qualities Scale. *Journal of Social and Personal Relationships* 11, 3: 471–484. https://doi.org/10.1177/0265407594113011

[12] Kathleen Carley. 1993. Coding Choices for Textual Analysis: A Comparison of Content Analysis and Map Analysis. *Sociological Methodology* 23: 75–126. https://doi.org/10.2307/271007

[13] Brian X. Chen. 2017. Google's New Parental Control App Has a Flaw: Puberty. *The New York Times*. Retrieved July 18, 2018 from https://www.nytimes.com/2017/07/26/technology/personaltech/android-parental-controls-family-link.html

[14] Anne Collier. 2014. Less parental control, more support of kids' self-regulation: Study. *ConnectSafely*. Retrieved July 18, 2017 from http://www.connectsafely.org/less-parental-control-more-support-of-kids-self-regulation-study/

[15] Lorrie Faith Cranor, Adam L. Durity, Abigail Marsh, and Blase Ur. 2014. Parents' and Teens' Perspectives on Privacy In a Technology-Filled World. In *Proceedings of the Tenth Symposium On Usable Privacy and Security*. Retrieved April 26, 2017 from https://www.usenix.org/conference/soups2014/proceedings/presentation/cranor

[16] Alexei Czeskis, Ivayla Dermendjieva, Hussein Yapit, Alan Borning, Batya Friedman, Brian Gill, and Tadayoshi Kohno. 2010. Parenting from the pocket: value tensions and technical directions for secure and private parent-teen mobile safety. 1. https://doi.org/10.1145/1837110.1837130

[17] Fred D. Davis. 1989. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly* 13: 319. https://doi.org/10.2307/249008

[18] Katie Davis, Anja Dinhopl, and Alexis Hiniker. 2019. "Everything's the Phone": Understanding the Phone's Supercharged Role in Parent-Teen Relationships. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (CHI '19), 227:1–227:14. https://doi.org/10.1145/3290605.3300457

[19] Katie Davis and Carrie James. 2013. Tweens' conceptions of privacy online: implications for educators. *Learning, Media and Technology* 38, 1: 4–25. https://doi.org/10.1080/17439884.2012.658404

[20] Nicola Dell, Vidya Vaidyanathan, Indrani Medhi, Edward Cutrell, and William Thies. 2012. "Yours is Better!": Participant Response Bias in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '12), 1321–1330. https://doi.org/10.1145/2207676.2208589

[21] Melanie M. Domenech Rodríguez, Melissa R. Donovick, and Susan L. Crowley. 2009. Parenting Styles in a Cultural Context: Observations of "Protective Parenting" in First-Generation Latinos. *Family Process* 48, 2: 195–210. https://doi.org/10.1111/j.1545-5300.2009.01277.x

[22] Sarah E. Domoff, Jenny S. Radesky, Kristen Harrison, Hurley Riley, Julie C. Lumeng, and Alison L. Miller. 2019. A Naturalistic Study of Child and Family Screen Media and Mobile Device Use.

Journal of Child and Family Studies 28, 2: 401–410. https://doi.org/10.1007/s10826-018-1275-1

[23] Matthew S. Eastin, Bradley S. Greenberg, and Linda Hofschire. 2006. Parenting the Internet. *Journal of Communication* 56, 3: 486–504. https://doi.org/10.1111/j.1460-2466.2006.00297.x

[24] Jenna Wharff Ed.M. Teaching Stranger Safety to Kids with Autism. Retrieved April 2, 2019 from http://blog.stageslearning.com/blog/teaching-autism-stranger-safety

[25] Lee B. Erickson, Pamela Wisniewski, Heng Xu, John M. Carroll, Mary Beth Rosson, and Daniel F. Perkins. 2016. The boundaries between: Parental involvement in a teen's online world. *Journal of the Association for Information Science and Technology* 67, 6: 1384–1403.

[26] Jieqiong Fan and Li-fang Zhang. 2014. The role of perceived parenting styles in thinking styles. *Learning and Individual Differences* 32, Supplement C: 204–211. https://doi.org/10.1016/j.lindif.2014.03.004

[27] Franz Faul, Edgar Erdfelder, Albert-Georg Lang, and Axel Buchner. 2007. G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods* 39, 2: 175–191. https://doi.org/10.3758/BF03193146

[28] Michela Ferron, Chiara Leonardi, Paolo Massa, Gianluca Schiavo, Amy L. Murphy, and Elisabetta Farella. 2019. A Walk on the Child Side: Investigating Parents' and Children's Experience and Perspective on Mobile Technology for Outdoor Child Independent Mobility. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (CHI '19), 597:1–597:12. https://doi.org/10.1145/3290605.3300827

[29] Karen L. Fingerman, Jacqui Smith, and Cynthia Berg. 2010. Coping and Self-Regulation across the Life Span. In *Handbook of Life-Span Development*. Springer Publishing Company.

[30] Batya Friedman, Peter H. Kahn Jr, Alan Borning, and Alina Huldtgren. 2013. Value Sensitive Design and Information Systems. In *Early engagement and new technologies: Opening up the laboratory*, Neelke Doorn, Daan Schuurbiers, Ibo Poel and Michael E. Gorman (eds.). Springer Netherlands, 55–95. Retrieved May 22, 2016 from http://link.springer.com/chapter/10.1007/978-94-007-7844-3_4

[31] Batya Friedman, Peter H. Kahn, and Alan Borning. 2002. *Value Sensitive Design: Theory and Methods*. Retrieved from http://faculty.washington.edu/pkahn/articles/vsd-theory-methods-tr.pdf

[32] Manuel Gámez-Guadix, Carmen Almendros, Erika Borrajo, and Esther Calvete. 2015. Prevalence and Association of Sexting and Online Sexual Victimization Among Spanish Adults. *Sexuality Research and Social Policy* 12, 2: 145–154. https://doi.org/10.1007/s13178-015-0186-9

[33] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph LaViola Jr., and Pamela Wisniewski. 2018. Safety vs. Surveillance: What Children Have to Say about Mobile Apps for Parental Control. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI '18).

[34] Arup Kumar Ghosh, Karla Badillo-Urquiola, Mary Beth Rosson, Heng Xu, Jack Carroll, and Pamela Wisniewski. 2018. A Matter of Control or Safety? Examining Parental Use of Technical Monitoring Apps on Teens' Mobile Devices. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI '18).

[35] Zhiwei Guan, Shirley Lee, Elisabeth Cuddihy, and Judith Ramey. 2006. The Validity of the Stimulated Retrospective Think-aloud Method As Measured by Eye Tracking. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '06), 1253–1262. https://doi.org/10.1145/1124772.1124961

[36] Richard HR Harper. 2014. *Trust, computing, and society*. Cambridge University Press.

[37] Heidi Hartikainen, Netta Iivari, and Marianne Kinnula. 2016. Should We Design for Control, Trust or Involvement?: A Discourses Survey About Children's Online Safety. In *Proceedings of the The 15th International Conference on Interaction Design and Children* (IDC '16), 367–378. https://doi.org/10.1145/2930674.2930680

[38] Yasmeen Hashish, Andrea Bunt, and James E. Young. 2014. Involving Children in Content Control: A Collaborative and Education-oriented Content Filtering Approach. In *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems* (CHI '14), 1797–1806. https://doi.org/10.1145/2556288.2557128

[39] C. Herodotou. 2018. Young children and tablets: A systematic review of effects on learning and development. *Journal of Computer Assisted Learning* 34, 1: 1–9. https://doi.org/10.1111/jcal.12220

[40] Alexis Hiniker, Sarita Y. Schoenebeck, and Julie A. Kientz. 2016. 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* (CSCW '16), 1376–1389.

[41] Saigeetha Jambunathan and Kenneth Counselman. 2002. Parenting Attitudes of Asian Indian Mothers

Living in the United States and in India. *Early Child Development and Care* 172, 6: 657–662. https://doi.org/10.1080/03004430215102

[42] Carrie James, Emily Weinstein, and Kelly Mendoza. 2019. Teaching Digital Citizens in Today's World: Research and Insights Behind the Common Sense K–12 Digital Citizenship Curriculum. *Common Sense Media*.

[43] MARGARET Kerr, HÅKAN Stattin, and KARI Trost. 1999. To know you is to trust you: parents' trust is rooted in child disclosure of information. *Journal of Adolescence* 22, 6: 737–752. https://doi.org/10.1006/jado.1999.0266

[44] Minsam Ko, Seungwoo Choi, Subin Yang, Joonwon Lee, and Uichin Lee. 2015. FamiLync: Facilitating Participatory Parental Mediation of Adolescents' Smartphone Use. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (UbiComp '15), 867–878.

[45] Claire B. Kopp. 1982. Antecedents of self-regulation: A developmental perspective. *Developmental Psychology* 18, 2: 199–214. https://doi.org/10.1037/0012-1649.18.2.199

[46] Jocelyn Lachance. 2019. Parental surveillance of teens in the digital era: the "ritual of confession" to the "ritual of repentance." *International Journal of Adolescence and Youth* 0, 0: 1–9. https://doi.org/10.1080/02673843.2019.1651351

[47] Susie D. Lamborn, Nina S. Mounts, Laurence Steinberg, and Sanford M. Dornbusch. 1991. Patterns of Competence and Adjustment among Adolescents from Authoritative, Authoritarian, Indulgent, and Neglectful Families. *Child Development* 62, 5: 1049–1065. https://doi.org/10.1111/j.1467-8624.1991.tb01588.x

[48] Simone Lanette, Phoebe K. Chua, Gillian Hayes, and Melissa Mazmanian. 2018. How Much is "Too Much"?: The Role of a Smartphone Addiction Narrative in Individuals' Experience of Use. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW: 101:1–101:22. https://doi.org/10.1145/3274370

[49] Richard S. Lazarus. 2000. Toward better research on stress and coping. *The American Psychologist* 55, 6: 665–673.

[50] Sonia Livingstone, Leslie Haddon, Anke Görzig, and Kjartan Ólafsson. 2011. *Risks and safety on the internet: The perspective of European children*. EU Kids Online. Retrieved from http://eprints.lse.ac.uk/33731/

[51] Sheri Madigan, Anh Ly, Christina L. Rash, Joris Van Ouytsel, and Jeff R. Temple. 2018. Prevalence of Multiple Forms of Sexting Behavior Among Youth: A Systematic Review and Meta-analysis. *JAMA Pediatrics* 172, 4: 327–335. https://doi.org/10.1001/jamapediatrics.2017.5314

[52] Monica Anderson. 2016. Parents, Teens and Digital Monitoring. *Pew Research Center: Internet, Science & Tech*. Retrieved September 10, 2018 from http://www.pewinternet.org/2016/01/07/parents-teens-and-digital-monitoring/

[53] Marije Nouwen, Nassim Jafarinaimi, and Bieke Zaman. 2017. Parental controls: reimagining technologies for parent-child interaction. https://doi.org/10.18420/ecscw2017-28

[54] Antti Oulasvirta, Aurora Pihlajamaa, Jukka Perkiö, Debarshi Ray, Taneli Vähäkangas, Tero Hasu, Niklas Vainio, and Petri Myllymäki. 2012. Long-term Effects of Ubiquitous Surveillance in the Home. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (UbiComp '12), 41–50. https://doi.org/10.1145/2370216.2370224

[55] R. Pain. 2006. Paranoid parenting? Rematerializing risk and fear for children. *Social & cultural geography.* 7, 2: 221–243.

[56] Sandra Petronio. 2015. Communication Privacy Management Theory. In *The International Encyclopedia of Interpersonal Communication*. American Cancer Society, 1–9. https://doi.org/10.1002/9781118540190.wbeic132

[57] Beate Rossler. 2018. *The value of privacy*. John Wiley & Sons.

[58] Diane J. Schiano and Christine Burg. 2017. Parental Controls: Oxymoron and Design Opportunity. In *HCI International 2017 – Posters' Extended Abstracts* (Communications in Computer and Information Science), 645–652. https://doi.org/10.1007/978-3-319-58753-0_91

[59] Daniel T. L. Shek. 2010. Parent-Adolescent Trust and Parent-Adolescent Relationships in Chinese Families in Hong Kong: Implications for Parent Education and Family Therapy. *The American Journal of Family Therapy* 38, 3: 251–265. https://doi.org/10.1080/01926180902945855

[60] Peter K. Smith, Jess Mahdavi, Manuel Carvalho, Sonja Fisher, Shanette Russell, and Neil Tippett. 2008. Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry and Allied Disciplines* 49, 4: 376–385. https://doi.org/10.1111/j.1469-7610.2007.01846.x

[61] H. Stattin and M. Kerr. 2000. Parental monitoring: a reinterpretation. *Child Development* 71, 4: 1072–1085.

[62] Laurence Steinberg, Susie D. Lamborn, Sanford M. Dornbusch, and Nancy Darling. 1992. Impact of Parenting Practices on Adolescent Achievement:

Authoritative Parenting, School Involvement, and Encouragement to Succeed. *Child Development* 63, 5: 1266–1281. https://doi.org/10.1111/j.1467-8624.1992.tb01694.x

[63] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. 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* (UbiComp '14), 129–139. https://doi.org/10.1145/2632048.2632107

[64] Pieter E. Vermaas, Yao-Hua Tan, Jeroen van den Hoven, Brigitte Burgemeestre, and Joris Hulstijn. 2010. Designing for Trust: A Case of Value-Sensitive Design. *Knowledge, Technology & Policy* 23, 3: 491–505. https://doi.org/10.1007/s12130-010-9130-8

[65] Angie Williams. 2003. Adolescents' Relationships With Parents. *Journal of Language and Social Psychology* 22, 1: 58–65. https://doi.org/10.1177/0261927X02250056

[66] Pamela Wisniewski, Arup Kumar Ghosh, Mary Beth Rosson, Heng Xu, and John M. Carroll. 2017. 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*.

[67] Pamela Wisniewski, Haiyan Jia, Na Wang, Saijing Zheng, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2015. 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* (CHI '15), 4029–4038. https://doi.org/10.1145/2702123.2702240

[68] Pamela Wisniewski, Haiyan Jia, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2015. "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* (CSCW '15), 302–316. https://doi.org/10.1145/2675133.2675293

[69] Pamela Wisniewski, Heng Xu, Mary Beth Rosson, Daniel F. Perkins, and John M. Carroll. 2016. Dear Diary: Teens Reflect on Their Weekly Online Risk Experiences. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (CHI '16), 3919–3930. https://doi.org/10.1145/2858036.2858317

[70] Jacob Wobbrock and Julie Kientz. 2016. Research Contributions in Human-Computer Interaction. *INTERACTIONS 23*, 38–44.

[71] Sarita Yardi. 2012. Social media at the boundaries: supporting parents in managing youth's social media use. Georgia Institute of Technology.

[72] Sarita Yardi and Amy Bruckman. 2011. Social and Technical Challenges in Parenting Teens' Social Media Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '11), 3237–3246. https://doi.org/10.1145/1978942.1979422

[73] 2018. It's Time to Do Something: Mitigating the Negative Impacts of Computing Through a Change to the Peer Review Process. *ACM FCA*. Retrieved January 6, 2020 from https://acm-fca.org/2018/03/29/negativeimpacts/

[74] Effects of Mobile Phones on Children's and Adolescents' Health: A Commentary - Hardell - 2018 - Child Development - Wiley Online Library. Retrieved September 20, 2019 from https://srcd.onlinelibrary.wiley.com/doi/full/10.1111/cdev.12831

[75] NSF Award Search: Award#1618153 - TWC SBE: Small: Helping Teens and Parents Negotiate Online Privacy and Safety. Retrieved January 6, 2020 from https://www.nsf.gov/awardsearch/showAward?AWD_ID=1618153&HistoricalAwards=false

[76] Kids want parental help with online risk, but fear parental freak outs. *ScienceDaily*. Retrieved September 18, 2018 from https://www.sciencedaily.com/releases/2017/02/170228084230.htm

[77] Amazon Rekognition – Video and Image - AWS. Retrieved June 10, 2018 from https://aws.amazon.com/rekognition/

[78] Client–server model - Wikipedia. Retrieved November 28, 2017 from https://en.wikipedia.org/wiki/Client%E2%80%93server_model

[79] Amazon Comprehend - Natural Language Processing (NLP) and Machine Learning (ML). *Amazon Web Services, Inc.* Retrieved June 10, 2018 from https://aws.amazon.com/comprehend/

[80] IBM SPSS Statistics 24 Documentation - United States. Retrieved June 18, 2017 from http://www-01.ibm.com/support/docview.wss?uid=swg27047033