

Parental Control vs. Teen Self-Regulation: Is there a middle ground for mobile online safety?

Pamela Wisniewski, Arup Kumar Ghosh

The University of Central Florida
College of Engineering and Computer Science
Orlando, FL USA

{pamwis, arupkumar.ghosh}@ucf.edu

Heng Xu, Mary Beth Rosson, John M. Carroll

The Pennsylvania State University
College of Information Sciences and Technology
University Park, PA USA

{hxu, mrosson, jcarroll}@ist.psu.edu

ABSTRACT

We conducted a structured, qualitative feature analysis of 75 Android mobile apps designed for the purpose of promoting adolescent online safety. Through this analysis we identified 42 unique features that mapped to a theoretically derived conceptual framework of teen online safety strategies balanced between parental control strategies (through monitoring, restriction, and active mediation) and teen self-regulation strategies (through self-monitoring, impulse control, and risk-coping). We found that the apps strongly favored features that promote parental control through monitoring and restricting teens' online behaviors over teen self-regulation or more communicative and collaborative practices between parents and teens. We use the lens of value sensitive design to discuss the implications of our results and identify opportunities for designing mobile apps for online safety that embed more positive family values.

Author Keywords

Adolescent online safety; parental control; teen self-regulation; mobile apps.

ACM Classification Keywords

K.4.1 [Public Policy Issues]: Ethics, Human safety, Privacy

INTRODUCTION

According to a Pew Research survey conducted in 2015, 91% of U.S. teenagers (ages 13 to 17) access the internet via a mobile device, enabling 92% of teens to go online daily [41]. Smart mobile devices allow teens to have easy and nearly constant access to the internet and social media sites. For instance, 47% of teens report using video chat applications ("apps" like Skype and Facetime), 33% use social messaging apps (e.g., Kik and WhatsApp), and 11% report using anonymous apps, such as Yik Yak and Ask.FM from their mobile devices [41].

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

CSCW '17, February 25-March 01, 2017, Portland, OR, USA

© 2017 ACM. ISBN 978-1-4503-4335-0/17/03...\$15.00

DOI: <http://dx.doi.org/10.1145/2998181.2998352>.

With this drastic rise in teen smart phone use, concerns about teen mobile online safety are also on the rise. The Crimes Against Children Research Center [46] estimates that most online risks teens encounter (e.g., exposure to unwanted explicit content, harassment, or sexual solicitations) are through the use of social media sites. Most concerning, however, is that a number of the social media apps teens use from their mobile devices have been associated with severe consequences ranging from illicit sexual exploits, teen suicide, and even murder [67,68]. As a response to this, social media coalitions, such as "Parents Who Fight" [69] have been popping up around the country to urge parents to find better ways to protect their teens from online risks. This demand has also led to a healthy market for parental control software designed to keep teens safe [70]. However, very little is known about the mobile apps currently available on the market for promoting adolescent online safety.

Therefore, we conducted an in-depth mobile app feature analysis of 75 Android apps that have the primary or secondary purpose of promoting teen mobile online safety. We identified 42 unique features that support both parents and teens in this goal with 382 instances of these features being supported across the apps in our data set. We also drew from developmental and cognitive psychology to create a framework of Teen Online Safety Strategies (TOSS) that conceptualizes the dichotomy between **parental control** and **teen self-regulation** in the context of adolescent online safety. We identified three primary parental mediation strategies (*monitoring*, *restriction*, and *active mediation*) and three analogous teen self-regulation strategies (*self-monitoring*, *impulse control*, and *risk-coping*) that could be leveraged in promoting adolescent online safety. We then mapped the various features identified in our feature analysis to our conceptual framework.

As a result, we found that the majority (89%) of the features identified supported parental control over teen self-regulation (11%). By-in-large these apps supported parental monitoring and restriction of teens' mobile activities. And, we found very few features in these apps that supported parental active mediation (<1%), teen risk-coping (4%), self-monitoring (2%), or impulse control (<1%). Educational features, however, emerged during our feature analysis and prompted us to add *education* as a fourth

online safety strategy for both parents and teens. We use the lens of *value sensitive design* [25,27] to discuss the implications of our results and suggest opportunities for the design of future mobile apps that promote adolescent online safety.

BACKGROUND

Adolescent Online Safety

While *adolescent online safety* is the broader topic associated with our research, we limited the scope of our background literature to adolescent online safety as it relates to *technical mediation* solutions. For a broader discussion about adolescent online safety and risks in general, see [11,14,32,34,35,62]. Technical mediation is defined as the use of software or applications to reduce teen online risk exposure and/or enforce appropriate online behaviors [22,43]. Traditionally, technical mediation has been considered a form of restrictive mediation [22] used by parents for filtering and/or monitoring content they deem inappropriate. A number of studies have examined adolescent online safety from the perspective of parental mediation through the use of parental control software [4,43,64]. However, the majority of these studies focus on in-home technical mediation, not of the use of technical mediation for mobile devices.

For example, in 2008 Livingstone and Helsper [43] found that technical restrictions did not have a significant effect on reducing exposure to explicit content (i.e., violence and pornography), information privacy breaches, nor contact-related risks (e.g., meeting an online stranger offline). Additionally, parents preferred non-technical parental strategies, such as co-use and rulemaking, over the use of technical restrictions. Only 33% of parents reported using filtering software and 23% had installed monitoring software. However, another 20% of parents were not even sure if they had such software installed on their home computers [43]. Yet in 2009, Ybarra et al. [64] found that parental control software installed on a home computer did effectively reduce the odds of a teen being exposed to unwanted sexual materials online by 65%. More recently, a 2016 survey conducted by Pew Research found that the use of parental control software on home computers is still relatively low (39%) [4] but did not address the effectiveness of using such technical parental mediation strategies to reduce teens' exposure to online risks.

Mobile Online Safety

In one sense, mobile online safety can be framed as a subset of adolescent online safety. However, we argue that mobile online safety may be even more salient and problematic due to three reasons. First, teens prefer to use mobile smart devices as a communication medium over more stationary devices, such as laptops or home computers. Second, these mobile devices give teens "near constant" access to the internet and social media [14,41]. Third, and most importantly, this seamless access to the internet is largely unmediated by parents because teens *literally* hold the

power (but possibly not the maturity) to connect at will, with anyone, and at any time in *the palm of their hands*.

Yet, the most recent Pew Research study [4] found that even fewer (only 16%) parents use parental controls on teens' cell phones compared to similar applications installed on home computers. Blackwell et al. [12] studied teens' use of mobile phones and social media and found that parents often underestimate how many and which social media apps teens use. Otherwise, very little research has examined the prevalence, strategies for, or the effectiveness of technical monitoring solutions used for mobile online safety. Instead, our literature search for related work uncovered a number of patents [1,13,15,44] and prototypes for mobile applications [2,30,37] that were designed to promote mobile online safety through technical mediation.

Amato et al. [2], developed a prototype leveraging computer vision to detect adult content from the images on a teen's phone. This approach taken from a computer science perspective was very similar to the advanced algorithms proposed by the various patents [1,13,15,44] for automatically and intelligently detecting unwanted and risky content on a teens' phone. However, the prototypes developed from more interdisciplinary fields tended to take vastly different approaches, by trying to find ways to involve teens *collaboratively* in the process of their own mobile online safety behaviors. For instance, Hasish et al. [30] developed an app for younger children (ages 6 to 8) called "We-Choose," which allowed parents and children to collaboratively configure mobile restrictions and filters. Their results suggest that this approach facilitated discussions between parents and children, making the process more enjoyable for both and giving parents greater insights into their children's notions of appropriate and inappropriate mobile content [30]. Similarly, Ko et al. [37] developed a prototype called "FamiLync" that used "participatory parental mediation" in which parents and teens engaged in activities that facilitated co-learning of digital media use. This participatory approach significantly increased the shared understanding of smartphone use, fostered positive parent-teen relationships, and encouraged active participation in use-limiting activities, which significantly reduced overall smartphone usage [37].

Research Contributions

What we have learned from the previous literature is, first, that the *existing* technical mediation solutions are generally *not* a preferred parental mediation strategy for promoting adolescent online safety in the home or through mobile devices. Second, there are *mixed* results as to their effectiveness even when in use. Third, the literature implies that *better* solutions need to be developed that are either more technically sophisticated or that promote more positive processes and outcomes, such as involving teens so that they are more engaged in decisions about their own mobile online safety. However, what we have not learned is *why* there is a gap between the technical mediation

solutions that currently exist and the new solutions proposed in the research that are not readily available for use.

Our main goal is, therefore, to better understand *why* this gap exists thereby targeting ways to effectively *close* the gap between the currently available technical mediation solutions for mobile online safety and the design of new solutions that better serve parents and teens. In this work, we make the following key contributions:

- 1) Developed a *conceptual framework* of Teen Online Safety Strategies (TOSS) presented in **Figure 1**. This was based on prior literature to provide a better theoretical understanding of the different strategies for mediating adolescent online safety.
- 2) Conducted a *feature analysis* of existing mobile apps to identify the mobile safety features that are currently supported. We describe this data coding process in our methodology.
- 3) Mapped the conceptual framework to the feature analysis to provide *descriptive details* and *emergent themes* related to the apps analyzed as our main results.
- 4) Identified *key implications* of our mapping, such as the values implied in the designs of these apps.
- 5) Proposed *design alternatives* for a new set of mobile online safety applications for teens and parents based on promoting more positive *family values*.

In the next section, we describe how we used the lens of value-sensitive design [25,27] and built a conceptual framework of mobile online safety strategies for adolescents.

CONCEPTUAL FRAMEWORKS

A Value Sensitive Design Approach

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” [25 p. 55]. VSD consists of a tripartite methodology of conceptual, empirical, and technical investigations that can both reflectively identify and proactively embed values that are of moral importance into the design of systems [26]. Conceptual investigations involve philosophical discussions about what values are, which values should be supported, and the design trade-offs among competing values. Empirical investigations study the human context in which a technology is used (e.g., user studies), while technical investigations focus on examining existing features within technology that may support or hinder human values [26]. Our work is, therefore, both a conceptual and technical investigation of the values embedded in the design of mobile apps that promote adolescent online safety.

While we apply the principles of value sensitive design in our work, we are not the first to leverage this approach in

the context of teen mobile safety. Czeskis et al. [18] used a value-sensitive design approach when they conducted scenario-based interviews with nine pairs of teens and parents regarding online safety to identify key technical challenges for design. They found that safety, trust, and privacy were salient values that caused tension between parents and teens and recommended design guidelines for addressing these tensions [18]. Unlike Czeskis et al. [18], our work intends to *reverse engineer* the values embedded in the design of *existing* mobile apps so that we can understand how they currently approach technical mediation for mobile online safety. By doing this, our goal is to understand the limitations of what is currently in use to better inform the design of new mobile safety solutions for teens.

In our work, we explicitly apply the lens of VSD to *family value systems*. Family systems are arguably the most important institution of modern society, and family values, which are socially constructed, become an integral part of who we are as humans and adults [33]. Family values are also contingent on a number of contextual variables, such as socioeconomic status [3,63], and shift over time [33]. The values ingrained into adulthood (e.g., obedience, discipline, honesty, transparency, trust, openness, etc.) also play a large role in how we parent [71]. For instance, a parent who values their teens’ privacy over their online safety may err on the side of indulgent parenting, while a parent who values the inverse may be more authoritarian in their parenting style [23]. However, research in developmental psychology confirms that authoritative parenting, where parents regulate and supervise teens’ behaviors but also are responsive and supportive toward their needs of individuality and autonomy, are most conducive to positive outcomes [23,58]. In the next section, we developed a conceptual framework of teen online safety strategies to illustrate this important balance between parental oversight and teen self-regulation.

Teen Online Safety Strategies Framework

Adolescent online safety is often framed as an outcome of effective parenting, which assumes that parents have some level of influence or control over teens’ exposure to online risks [20,36,40,43]. However, prior literature also suggests that tension exists between parental control and teen autonomy when it comes to teens’ online behaviors, their desire for privacy, and online safety [14,23,48,49]. Our background literature also highlighted the importance of collaborative practices that involved teens in their own mobile safety [18,30,37]. Therefore, the two main strategies we included in our conceptual framework of Teen Online Safety Strategies (TOSS) are parental control and teen self-regulation. In the sections that follow, we further define parental control and explain how *monitoring*, *restriction*, and *active mediation* are three primary ways in which parents can influence teen online safety. We also discuss teen self-regulation and three of its key components – *self-awareness*, *impulse control*, and *risk-coping*.

Parental Control

Much of the original work regarding parental mediation strategies for online safety was originally derived from Valkenburg et al.'s [57] scale assessing three styles of parental television mediation: social co-viewing (i.e., monitoring), restrictive, and instructive (i.e., active) mediation. These constructs and scales have since been adapted for use in the context of online parental mediation [20,22,43,45]. We will define and briefly discuss some of the literature related to each of these parental mediation strategies.

Monitoring

Monitoring is defined as the surveillance of a teen's online activities, such as checking text messages, call logs, or web browser history [42]. Monitoring is often considered a more passive parental mediation strategy, where a parent either co-views the content being consumed (e.g., a web page) or checks logs to monitor teens' activity after-the-fact. For instance, nearly half (48%) of parents in the Pew Research study said that they manually checked the teens' call log or text messages from their mobile devices [4]. Mesch [45] found that monitoring websites visited reduced the cyberbullying risks posed to teens. However, other research has found that parenting monitoring was actually associated with *higher* levels of online risks for some teens [20], suggesting that monitoring may occur after teens have already experienced some kind of problem online.

Restriction

Restrictive mediation occurs when parents place rules and limits on a teen's online activities [22,42]. Examples of rules include setting limits on screen-time or the types of content deemed acceptable for viewing [57]. Mesch [45] found that creating rules for what websites teens could visit also reduced cyberbullying. However, Shin and Ismail [52] suggest that "control-based" parenting through restrictive mediation may have negative effects, causing teens to take more risk-seeking behaviors, such as becoming friends with strangers on social networking sites.

Active Mediation

Active mediation involves interactions and discussions between parents and teens regarding online activities or experiences [22,42]. This parental mediation strategy has been used synonymously with "evaluative" or "instructive" mediation [57]. In the context of television viewing, active mediation occurs when parents discuss how "certain shows are unrealistic, or that good or bad things are done by characters" [57 p. 3]. Similarly, parents have numerous opportunities to discuss the often inappropriate content teens may consume online [62]. Duerager and Livingstone [20] suggest that active mediation may reduce online risks without reducing potential benefits of online engagement. Wisniewski et al., [60] also found an "empowering" effect of active mediation where teens were able to engage in online activities and get help from their parents when they found themselves in riskier situations.

Teen Self-Regulation

Not much work has been done in the realm of teen-self regulation and online safety. However, recent work by Wisniewski et al. [59], suggests that teens can exhibit resilience that serves to protect them from negative effects of the online risks they encounter. And, when teens encounter online risks, they often take active measures to cope with them [62]. As such, we went back to the adolescent developmental psychology literature and found that self-regulation can be framed as a "resiliency factor" in protecting teens from deviant peer influences and anti-social behavior [28]. **Self-regulation** is defined as the ability to modulate one's own emotions and behaviors through monitoring, inhibiting, and evaluating oneself compared to given societal standards [24,38,47]. Bi-direction influences have been found between patterns of parental mediation strategies and teen self-regulatory behaviors [47]. Therefore, we incorporated teen self-regulation into our framework and drew from the developmental psychology literature in the sections below.

Self-Monitoring

According to social cognitive theory, "most human behavior, being purposive, is regulated by forethought" [6 p. 248]. Therefore, **self-monitoring** is a key component of self-regulation [6,38]. However, in relation to teens, research has often found that such self-monitoring and regulatory "forethought" may be lacking [53,54], which is why teens may have a higher proclivity towards risk-taking. In order for teens to effectively self-regulate their own online behaviors, they must be aware (at least to some level) of their own motivations and actions through self-observation [6]. Therefore, we include this as one of the teen self-regulation strategies in our conceptual framework.

Impulse Control

Impulse control is defined as the ability to inhibit one's short-term desires in favor of the long-term consequences that may be caused by one's actions [10]. Losing control of one's short-term desires or impulses has been cited as one of the major reasons why self-regulation fails [7] and has been linked to a higher-order construct of executive functioning [28]. Again, research suggests that impulse control is "relatively immature" in teens and may lead to "suboptimal decisions" [16]. However, we include impulse control in our TOSS framework because it can act as a protective mechanism for online risks.

Risk-Coping

Coping is related to self-regulation in that it is a self-regulatory process that occurs *after* one encounters a stressful situation [24,39]. It involves both attempting to address the problem and managing the negative emotions that are caused by the event [24]. Adolescent developmental psychology literature has identified two main dimensions for coping strategies, which include approach and avoidance/withdrawal [21,51]. Approach strategies involve more active processes, such as problem-solving, advice-seeking, and acquiring social support.

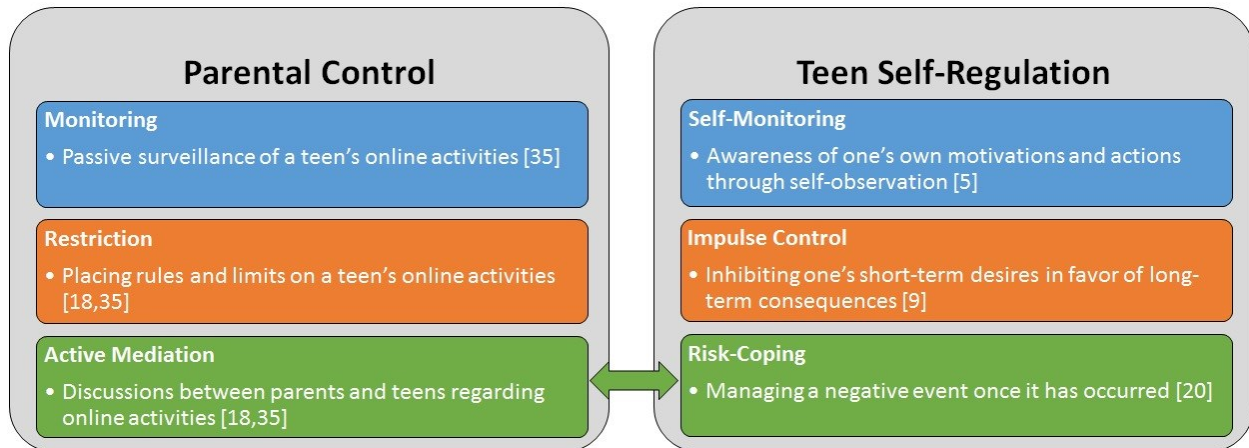


Figure 1: Teen Online Safety Strategies (TOSS) Conceptual Framework

Avoidance strategies are considered more passive or fatalistic, where teens attempt to withdraw from the problem without trying to change or improve it. Some adolescent online safety literature has already addressed the importance of risk-coping [19,34,60], finding that risk-coping is influenced by both parental mediation strategies and the teens' own appraisals of their online risk experiences. Actively coping with risky online situations has been found to help teens feel less bothered about the event that occurred [19]. Thus, the risk-coping literature [34,60] ties directly back to the concept of building teen resilience [59] so that teens can thrive in spite of experiencing online risks [60].

In summary, we developed a theoretically derived framework of Teen Online Safety Strategies (TOSS) (Figure 1) that includes both strategies for parental control and teen self-regulation. We visually situate the parental strategies with the analogous teen strategies (e.g., parental monitoring versus self-monitoring) for online safety, and we show an explicit relationship between parental active mediation and teen risk-coping. This is because when teens experience risk, one of the ways they can cope is by seeking active mediation or help from their parents [60]. We will apply this framework to the domain of mobile online safety to understand the feature sets that support each of these strategies. We describe how we did this in our methods section below.

METHODS

Data Collection

In April through May of 2016, we conducted a structured analysis of Android mobile applications ("apps") that promote adolescent online safety and are currently available for download via Google Play. We chose to focus on the Android platform because it currently has 83% of the global market share for mobile smartphones [72]. We discuss the constraints of this decision in more detail in our limitations section. In our analysis, we focused on apps that were

designed for the primary purpose of adolescent online safety but included some apps that could easily be used for online safety as a secondary purpose. Only apps that were free or had a free-trial were included in this analysis. We did not include apps that wanted us to provide our credit/debit card details for using their trial versions. We excluded apps designed specifically to monitor teens' physical location (e.g., GPS tracking) unless they also included features of online safety.

Given the above criteria, we first performed a keyword search on the Google Play app store using the terms "online safety," "family safety," "teen safety," "adolescent online safety," "parental controls," "parental monitoring," "teen monitoring," "cyberbullying," and "sexting." These keywords were chosen because they were consistent with the risk terminology in the prevailing adolescent online safety literature [46], and more importantly, because they did not limit the search only to parental control software. We read the Google Play descriptions to determine if the apps met our inclusion criteria above. If so, the name of the app was recorded for later analysis. We then examined all "similar" apps that were suggested by Google Play for all of the apps that were found in our initial search.

We repeated this process until we had reached a point of saturation such that no new apps were identified as relevant for inclusion. Through our iterative search process, we generated an initial list of 89 apps. Out of these 89 apps, we removed 14 apps upon installation. This was due to 3 apps that required payment information to use the trial version, 4 that were installed but did not work properly, 1 that was targeted only to teachers and required payment, 2 that applied only within a particular school district, 1 that was only for Verizon users, and 3 that were helper apps for apps already included in our analysis. Therefore, our final data set included 75 apps.

Data Analysis

We used a combination of a *top-down* and *bottom-up* approach to qualitatively analyze our data. First, we leveraged existing theory to create the conceptual TOSS framework of the different strategies that parents and teens could employ to keep teens safe online. We believe that this framework is valuable because it can be generalizable to other contexts within adolescent online safety beyond mobile online safety. Then, we used a grounded approach [56] to compile a list of all the different features available within the 75 apps in our sample.

We conducted our feature analysis by installing each app one-by-one on an Android mobile phone and exploring all of the available features. The phone used for the analysis was a Google Nexus 5X [73] with 16 GB of storage running the Android 6.0 Marshmallow [74] operating system. If a particular feature had not yet been recorded in the spreadsheet, we created a new column for this feature (e.g., website monitoring, website blocking, etc.). If the feature had already been created from a previous app analysis, we updated the coding scheme for the new app to reflect whether the feature was present or not (i.e., “Yes,” “No”). After the initial coding was complete, an iterative round of coding was performed to provide more detailed information for features that were present. For example, for features associated with monitoring, we created additional codes for whether parents had access to low-level data (e.g., all browser history, text messages, etc.), summary data only (e.g., types of websites browsed, count of incoming and outgoing text messages), or both.

The feature analysis data coding was performed by two research assistants who sub-divided the apps. Cohen’s kappa was calculated to ensure inter-rater reliability (IRR) [29] on a hold out sample of 20% of the data (15 apps). Through the data coding process, we were able to inductively create a comprehensive list of all of the mobile app features currently available for promoting adolescent online safety. We identified 42 unique features for parents and teens within the 75 mobile apps. This included 382 instances where a feature was available within an app. Note that the relationship between features and apps is many-to-many; a single feature may be present in multiple apps, while an app may support multiple features.

Finally, we mapped the set of features (bottom-up) to our conceptual framework (top-down) in order to integrate theory building (e.g., feature analysis) with our conceptual TOSS framework. The results of this mapping, as well as the IRR for each coded feature are summarized in **Appendix A, Table 5**. In most cases, each feature logically mapped to one or more of the dimensions in the conceptual framework with the exception of one feature that emerged: *educational features*. Therefore, education was added as a fourth strategy for adolescent online safety for both parents and teens. It is through this over-arching conceptual TOSS framework that we will present our results. We also include a section in our discussion that focuses on the usability

issues that we discovered when installing and exploring the mobile apps. All of the apps included in our analysis are listed in **Appendix A, Table 6**.

Descriptive Statistics

Of the 75 apps, 49% had interactive interfaces only for parents, 49% provided interfaces for both parents and teens (though extremely limited for teens), and only 1% were applications specifically for teens. In most cases, the apps were designed to be installed on a teen’s mobile device to run in the background so that parents could remotely monitor and restrict mobile activities performed via the device. A companion app, website, or notification system were used so that parents could monitor their teens’ mobile activities and/or set restriction levels on mobile use. MamaBear Family Safety, MMGuardian Parent App, and Bitdefender Parental Control are examples of apps, which provided interfaces for both parents and teens. A common theme among these types of apps, however, is that the features available to teens were significantly limited compared to those available to parents. For instance, 41% of these apps only had seek-help features for teens to use in the case of an emergency. Further, it was rare to find an app that was designed just for teens. ReThink - Stops Cyberbullying was the only app and was developed by a 15-year-old teen for the purpose of reducing cyberbullying at the source [66].

The majority (60%) of the apps were targeted toward both children and teen online safety while 24% of the apps were geared more toward younger children than teens, 9% adults, only 3% teens, and 4% were unspecific as to their target. Apps for younger children often included games for teaching online safety and launcher apps to protect a parent’s phone while used by a child. Apps targeted toward adults included accountability apps, such as Ever Accountable, which was designed to help combat adult porn addictions but could also help teens from exposure to explicit content. Since these apps could potentially be used for the secondary purpose of adolescent online safety, we chose to include them in our analysis for the sake of completeness. As such, online safety was the primary purpose for 73% of the apps with 27% having another primary purpose. For example, Cerberus anti-theft provided features, such as active monitoring of the mobile device, but it was targeted to anti-theft purposes, not specifically to teen online safety.

In terms of cost, 59% of the apps were free for download while nearly a quarter (24%) only provided a limited-time trial version. In most cases, the free trial expired after a period of one week to 30 days. Another 16% of the apps provided both a free and paid version. In these cases, the free version supported basic features while the paid version gave users additional functionality.

RESULTS

As shown in **Figure 2**, the majority (89%) of the features (N=382) identified to support online safety were targeted

toward parents with only 11% of the features supporting some form of teen self-regulation. The parental control strategies most supported by the feature set included monitoring (44% of features), restriction (43%), and education (2%). Parental active mediation was supported by less than 1% of the features. For teen self-regulation, the primary strategies for online safety included risk-coping (4%), self-monitoring (2%), and educational features (4%). Impulse control was identified in less than 1% of the features found during our analysis.

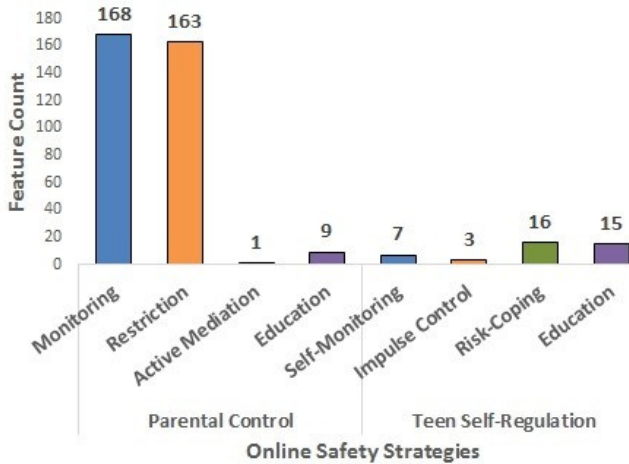


Figure 2: Supported Features (N=382) by TOSS Framework

Parental Mediation and Control

Monitoring

Monitoring was the most widely supported TOSS feature across the 75 apps, with 44% of the features identified among all apps supporting parental monitoring and 64% of apps having at least one parental monitoring feature. **Table 1** summarizes the features that supported parental monitoring and the percentage of apps that supported each feature. Please see **Appendix A, Table 5** for more descriptive definitions of each of the features presented in our results.

Table 1: Parental Monitoring Features

FEATURES	% APPS (N = 75)
REPORTING	59%
BROWSER-LOG	37%
APP-LOG	31%
LOCATION-LOG	29%
TXTMSG-LOG	27%
CALL-LOG	25%
SCREENTIME-LOG	8%
SOCMED-LOG	8%

Over half (59%) of the apps in our data set included reporting features where mobile activity logs could be either sent (i.e., “pushed,” 21%) or retrieved (i.e., “pulled,” 37%) to parents. Although we coded for the possibility of

monitoring at the connection-level (i.e., data, Wi-Fi, Bluetooth, or other connection) or keyboard-level, we did not find any apps that supported these types of features for parents.

We then created sub-codes for the level of detail provided to parents through the logs that monitored teens’ mobile activities. *Details* meant that the parent received all low-level details, such as the URL of the website browsed, content of each text message, or the exact location of a teen. *Summary* meant that the parent only received aggregated meta data regarding the activity, such as the time spent browsing or how many text messages were sent or received. *Both* meant that the parent could monitor both the details and get aggregated reports on the teen’s activity. A common theme that we found across all of the monitoring features was that summary-only monitoring was very uncommon, ranging between 0 to 3% of all apps. Instead, when monitoring was supported, the design of the apps favored full disclosure (e.g., *Details*). For example, a number of apps allowed the parent to read each text message sent and received by the teen. These apps included ShieldMyTeen Parental Control, TangTracker e-Safety App, and others.

Restriction

Parental restriction was the second most supported TOSS based on the feature set. A total of 32% of the features identified across all apps supported restriction with 65% of apps having at least one feature that supported parental restriction. Web browsing and app-level blocking were the most commonly supported restrictive features, followed by restricting screen-time. We also coded for the potential for parents to actively regulate keyboard-level activities, but no apps supported this feature. **Table 2** summarizes the apps and features that supported parental restriction.

Table 2: Parental Restriction Features

FEATURE	% APPS (N = 75)
BROWSER-BLOCK	60%
APP-BLOCK	52%
SCREENTIME-BLOCK	44%
CALL-BLOCK	28%
TXTMSG-BLOCK	21%
SOCMED-BLOCK	9%
CONNECT-BLOCK	3%

We created another set of sub-codes to describe features used actively regulate teens’ online behaviors. *All* meant that the feature supported blocking of activities overall, while *some* indicated that parents could contingently allow certain activities and restrict others. Generally, we found that the most supported features (e.g., restrictive browsing and app activity) supported more options for filtering than the less frequently implemented features in the apps. For

example, 93% of apps that supported restrictive browsing allowed parents to pick and choose specific sites to filter.

Active Mediation

Active mediation had the weakest support with only one app having a feature to support this strategy. In SafeKiddo Parental Control, teens request access to specific apps or to use their device once their time limit has expired. Parents are able to actively mediate through the app by allowing or denying such requests.

Educational Features

Although not originally included in our TOSS framework, educational features emerged from our grounded feature analysis as a fourth strategy for promoting adolescent online safety – for both parents and teens. Nine apps provided instruction to parents for protecting their teens online. Internet Safety is one such app, which upon installing is a digital book on online safety. WOT Mobile Security provides parents and teens a reference guide for trustworthiness of websites. Educational apps also included games and other instructional media, which we will describe further in the teen strategies for educational online safety.

Teen Self-Regulation

Self-Monitoring

Teen self-monitoring was poorly supported as only 9% of apps (7 apps) had features that supported this strategy. Of these features, the most frequently supported feature (still only 5% of apps) was sending reports to teens about their online activities. This feature was supported by four apps - Ever Accountable, Accountability Soft, Mobile Fence Parental Control, and MamaBear Family Safety. Two of these apps were accountability software aimed at reducing adult pornographic exposure. Two were parental monitoring apps that gave teens minimal summary views as to their mobile activities. We also reviewed apps for any features related to teen self-monitoring of keyboard-level activities, location, screen-time, text messaging, call logs, and social media activity but did not find any apps that supported these features for teens. **Table 3** summarizes the apps and features that supported teen self-monitoring.

Table 3: Teen Self-Monitoring Features

FEATURES	% APPS (N = 75)
REPORTING-T	5%
CONNECT-LOG-T	1%
APP-LOG-T	1%
BROWSER-LOG-T	1%

Impulse-Control

Teen impulse control also was weakly supported with only three apps that featured this teen self-regulation strategy. ReThink - Stops Cyberbullying helped teens make better decisions regarding the messages that they sent to others in an attempt to reduce mean-spirited messages from being sent. This was done through a keylogging program that

detected potentially malicious sentiments in the teens’ written text. The other two apps had minimal settings so that teens could disconnect their device from data services or block websites. We coded for apps that supported teen impulse control related to apps, calls, screen-time, text messaging, and social media but no apps were identified. **Table 4** summarizes the apps and features that supported teen self-monitoring.

Table 4: Teen Impulse Control Features

FEATURE	% APPS (N = 75)
BROWSER-BLOCK-T	1%
CONNECT-BLOCK-T	1%
KEYBOARD-BLOCK-T	1%

Risk-Coping

Teen risk-coping was the strongest supported strategy for teen online safety with 20% of the apps being coded as having features to support this strategy. Of these 16 apps, 15 of them provided an “SOS” feature so that teens could seek help from their parents, an organization, or emergency services. Only one app, SafeKiddo Parental Control, which was mentioned earlier in regard to parental active mediation, gave teens the ability to negotiate their online safety practices with their parents.

Educational Features

We identified 15 apps (20% of the apps) that were designed with the purpose of educating teens about online safety. For instance, bCyberwise Monster Family gamified internet safety. Happy Onlife similarly taught younger kids (ages 8-12) about online safety, though could be used by teens. Discovery Schools Trust, KidzSearch App were some other apps which had educational features for teens. A key distinction between the educational apps and the other online safety apps is that they were often mutually exclusive, not including addition parental control or teen self-regulation support.

DISCUSSION

In summary, we conducted a feature analysis of 75 Android mobile apps that have the primary or secondary purpose of promoting adolescent online safety. We found that the overwhelming majority (89%) of the apps supported parental control strategies over strategies for teen self-regulation with the focus on parental monitoring (44%) and restrictive mediation (43%) of teens online activities. However, there was also a decent percentage of apps (6%) that supported educational strategies for helping teach parents and teens about online safety.

Figures 3 & 4 further summarize our findings for parental mediation and teen self-regulation strategies as they directly relate to the activities teens engage in via their mobile devices. As shown in **Figure 3**, web browsing was the most frequently mediated mobile activity with 37% of apps allowing parents to monitor web browsing history and 60% providing ways for parents to restrict access to websites.

App-level parental mediation was the second most prevalent activity supported with 52% of apps offering ways for parents to restrict app-level access and 31% allowing parents to monitor the apps teens installed on their mobile devices. Keyboard (0 apps), data connection (2 apps), and social media (6-7 apps) activities were among the lowest in terms of apps that facilitated parental monitoring and restriction of their teens' mobile activities at these levels.

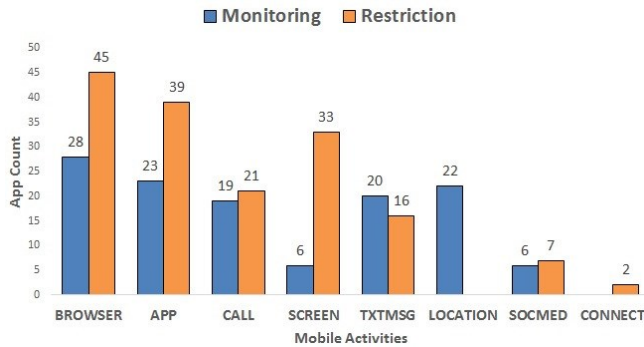


Figure 3: Parental Controls by Teen Mobile Activities

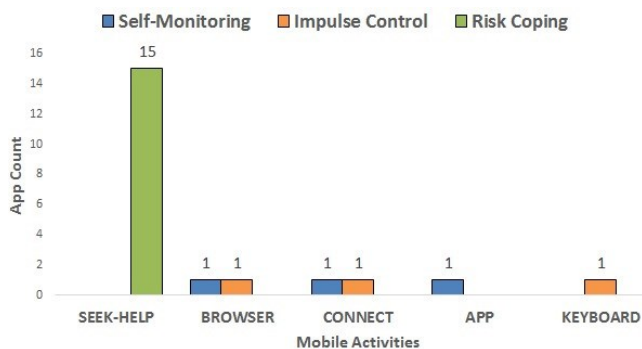


Figure 4: Teen Self-Regulation by Mobile Activities

Figure 4 illustrates the apps that supported teen self-regulation of their own mobile activities. Overall, we found very few apps that helped teens self-monitor or otherwise regulate their own mobile activities. Instead, apps that supported teen self-regulation tended to do so by offering teens an SOS feature so that they could seek help from others in the event of an emergency, which, in its simplest form, would be considered a type of risk-coping. These findings present a number of insights, as well as opportunities for design that we will discuss in the sections below.

Looking through the Lens of Value Sensitive Design

One of the central tenets of VSD is understanding the stakeholders who may be directly and indirectly impacted by a technology and the trade-offs that must be made in design between upholding the values of one stakeholder over another [25]. Based on our results, we can infer some of the values and trade-offs inherent in the design of the existing mobile apps for teen online safety. First, *parental authority* and *teen safety* are valued over *teen autonomy*

and their *personal privacy*. [9]. Such results suggest a strong preference on supporting parents as primary stakeholders over teens. Some of the app publishers even explicitly acknowledged this imbalance in their market descriptions:

“Your children will hate us for publishing this Child Safety Online apps and making it available for free. Send our apology to them but as an adult, their safety is more important and we are here with the intention to help.” – Child Safety Online [75]

Additionally, parental control through *privacy invasive monitoring* and *restrictions* was valued over having *open communication* with teens through features that support *active mediation* strategies. We only found one app that had built in negotiation features to allow parents and teens to interactively set boundaries regarding appropriate online behaviors. Otherwise, many of the apps felt as if they were more like Trojan horses, designed to covertly run on a teen’s phone to spy on and block the mobile activities that their phones were natively designed to support. In this way, the apps made teens’ mobile devices *less* useful for them, albeit more “safe.” The lack of teen-focused features and associated value propositions ignores teens as stakeholders in the design process, and thus, makes them forced, as opposed to willing, users of parental control apps. As a result, we observed teens who left negative app reviews, which deflated some app ratings. Yet, the app company below used the negative feedback from teens as a way to further rationalize the value of their app:

*“**Negative reviews of TeenSafe Child are coming from the children of parents using TeenSafe, not the parents themselves. We think these negative reviews are proof that TeenSafe works.**” –TeenSafe Child [76]*

From a teen self-regulation perspective, *asking for help* was valued over trying to *actively cope* with the problem oneself. This implied that teens were seen as incapable of being the agents of their own online safety. Generally, “positive” family values [18] were *enforced* for teens by the apps that exposed the transparency of their actions, forced obedience, and enacted behavior modulation so that parents could “trust” that their teens were safe – as opposed to aiding self-regulatory processes so that teens could embody these values on their own. This negates the more resilience-based approaches advocated in recent adolescent online safety literature [34,59,60,62] that support allowing teens to engage in some level of online risk so that they can learn from their mistakes, develop effective coping mechanisms, and protect themselves from online risks.

To conclude this section on a more positive note, *knowledge* was also a key value implied in the design of a number of the apps. These apps provided educational tools to teach parents and teens how to engage online safely.

Issues Concerning Usability

One of the goals set forth in our research was to develop a clearer understanding of the mobile apps currently available

on the market for promoting adolescent online safety, as well as understanding their limitations. After installing and trying to use these apps, usability issues were a strong emergent theme from our analysis that we could not ignore. Originally, we identified 89 apps that were relevant during our search. However, due to issues upon installation, we were unable to analyze 14 of these apps. Many apps we did analyze required considerable efforts upon start-up, such as Phone Tracker, which required users to have a Gmail account, and Verizon FamilyBase, which needed a Verizon connection for registration. Safe Browsing Parental Control needed the user to configure a VPN connection. Other parental control apps required us to install companion apps on another phone (i.e., teen's phone). These included MMGuardian Parent App, FamilyTime - Parental Control, and Trackidz (Parental Control). A number of other apps had annoying ads, which made exploration more difficult. Parental Control Launcher and Parental Control and Dashboard are two examples. X3Watch kept trying to bring us to the xxxchurch.com website.

Other apps, such as Accountable2You and Covenant Eyes, were misleading because they were free for download but upon opening them after installation, they required a credit card number. NetSpark Parental Control also had similar conditions for their trial version but they at least disclosed this in their description on Google Play. Finally, after installing and then uninstalling all 89 apps, on the Android device, the phone would no longer accept calls and was rendered unusable. Even though these usability issues are orthogonal to our primary lens of VSD, they are worthy of mention because they create additional barriers for adoption and use, especially for parents who may lack the technical prowess [23] to deal with these types of issues.

Practical Implications for Parents and Teens

Through our analysis, we uncovered three potential reasons why technical mediation solutions for mobile online safety are only used by a minority of parents (16%) [4]. These include 1) difficulties in finding and using the apps, 2) the features within these apps not meeting the goal of protecting teens from the online risks they encounter, and 3) being incongruent with family values. We will discuss these implications in further detail below.

The usability issues we summarized earlier, as well as the difficulty in identifying apps that serve the purpose of promoting adolescent online safety, may likely contribute to the under-utilization of these apps. Very few apps explicitly said that they were designed for teen online safety, often trying to appeal to a broader audience of parents who had children and/or teens. Other apps were targeted toward completely different audiences, such as young children and adults, even though they could be used in the context of teen online safety. In contrast, some of the apps that came up through our search results would actually *encourage* deviant behaviors, such as one app that was targeted toward cheating adults, but would allow teens to send secret messages and create hidden contacts. Our search terms also

yielded a number of apps that were clearly *not* relevant upon reading their descriptions. These included anti-virus software, games, and spying apps. The inability to locate relevant apps, usability issues, and the digital divide between parents and teens in terms of technology savvy [23], all may contribute to problematic use cases for these apps that help explain low adoption rates.

Next, the features within these apps did not fully meet the goal of protecting teens from the online risks that would be most detrimental to their safety. Research suggests that most adolescent online risks are encountered through the use of *social media* platforms [46,62]. Yet, in terms of the mobile activities monitored or restricted by these parental control apps, web browsing was the most prevalent and social media regulation was one of the least (**Figure 3**). Instead, these apps tried to address the problem at the app-level, giving parents control over what apps teens can install or open from their mobile devices, making social media participation an all or nothing decision. This design decision may be due to technical feasibility constraints associated with gaining access to social media APIs, but from a practical standpoint, these features did not adequately address the most pressing problems teens face as they use mobile social media apps to engage with others.

Finally, the features offered by these apps generally did not promote values, such as trust, accountability, respect, and transparency, that are often associated with more positive family values [18]. Simply put, the values embedded within these apps were incongruent with how many parents of teens want to parent. For instance, Eastin et al. [22], compared parental mediation strategies for online safety across the four classic parenting styles – authoritarian, authoritative, indulgent, and neglectful parenting [8,55]. They found that technical mediation was highest among authoritative followed by authoritarian then neglectful parents. In this case, parents who are more indulgent (not demanding of their teens' behavioral compliance and highly responsive for their teens' need for autonomy [8,55]) would not be willing to use such restrictive and privacy-invasive parental control apps. In contrast, authoritative parents, who were found to be the most frequent adopters of technical mediation solutions, are parents who want to balance being actively engaged in their teens' online activities while still giving them opportunities to engage online with others. Unfortunately, the apps in our analysis rarely supported such active, engaged, and supportive parenting and would, therefore, ultimately not meet the needs of these more authoritative parents in the long-term.

Opportunities for Design

With a better understanding of the portfolio of features currently available for mobile online safety, as well as the values implied by the design of these features, we can begin to suggest a subset of new design practices and features that promote alternative values. First, by using the lens of VSD, it becomes very clear that teens need to be included in the design of apps that are created to protect their online safety.

For the apps we analyzed, it seems likely that teens were not involved in design or that the unintentional biases [50] of the creators overly influenced design decisions. For example, some of the apps were actually designed or developed by parents who wanted to keep their teens safe. Thus, the features were probably more focused on parental desires than those of teens'. Instead, we need to find better ways of using principles of interaction design that respect the needs, challenges, and opportunities that are unique to teens, not just parents [50]. Some recent research has begun this process by using participatory design methods with teens to reduce addictive cell phone usage [37] and address cyberbullying [5]. Given the positive results found, we suggest more research follow their direction.

Beyond involving teens in the design process, it is important to also change the use cases by which we design solutions for mobile online safety. **Figure 5** illustrates the current way (left) parental control apps protect teens compared with our newly proposed framework (right), which visualizes a VSD approach to the TOSS framework. On the left, current solutions are fairly simplistic; as new mobile functionality becomes available, new apps must be created so that parents can remotely monitor and regulate the mobile activities of teens. Thus, the relationship is fairly one-to-one; as new interactive features are introduced, new preventative ones are developed. However, an inherent flaw in this model is that new interactive technologies will *always* outpace the ones developed to shield teens from risky interactions. For instance, apps such as Snapchat [65] challenge parents and designers to find effective ways to prevent teens from the lure of seemingly ephemeral sharing, which may promote inappropriate behaviors (e.g., sexting or cyberbullying). Further, such solutions may prevent risks, but they do so at the expense of also limiting potential opportunities to engage with others.

On the right, we propose a new framework for designing

and developing mobile online safety apps that is founded on core family values, whatever those may be, and emphasizes parental active mediation and teen self-regulation (**Figure 1**), which are currently under-supported in current offerings. A benefit of this framework is that features need *not* be technically tied directly to teens' mobile activities, and can, therefore, focus on supporting more important, yet intangible, needs of parents and teens. Our framework, for instance, supports the earlier approaches cited in our background literature [30,37], where the authors proposed mobile app prototypes to promote collaborative practices between parents and teens that support both teen risk-coping and active parental mediation. These types of collaborative efforts between parents and teens are certainly an uncharted territory that should be further explored.

Supporting teen self-regulatory processes in the *absence* of parents is another area that presents a unique opportunity for design. For instance, instead of simply giving teens an SOS feature to get help from adults, we might find ways to more meaningfully support teen risk-coping, so that they can come up with their own solutions to online problems or to come to the aid of other teens who could benefit from their help. Additionally, how could we help teens be more self-aware and use that awareness to make better decisions (e.g., impulse control)? As an example, the native functionality of a mobile device provides raw data such as call logs, app usage (via battery usage), browser history, etc., but the design challenge is interpreting this data into useful knowledge that teens could leverage to modify their own behaviors. As another example, Amato et al.'s [2] app prototype used computer vision to detect sexually explicit imagery on teens' mobile devices. An alternative approach to using risk detection as a means to block content or notify parents would be to use this information to gently "nudge" teens toward more appropriate behaviors [35]. However, before implementing self-monitoring and impulse control features, we would need to first determine what behaviors

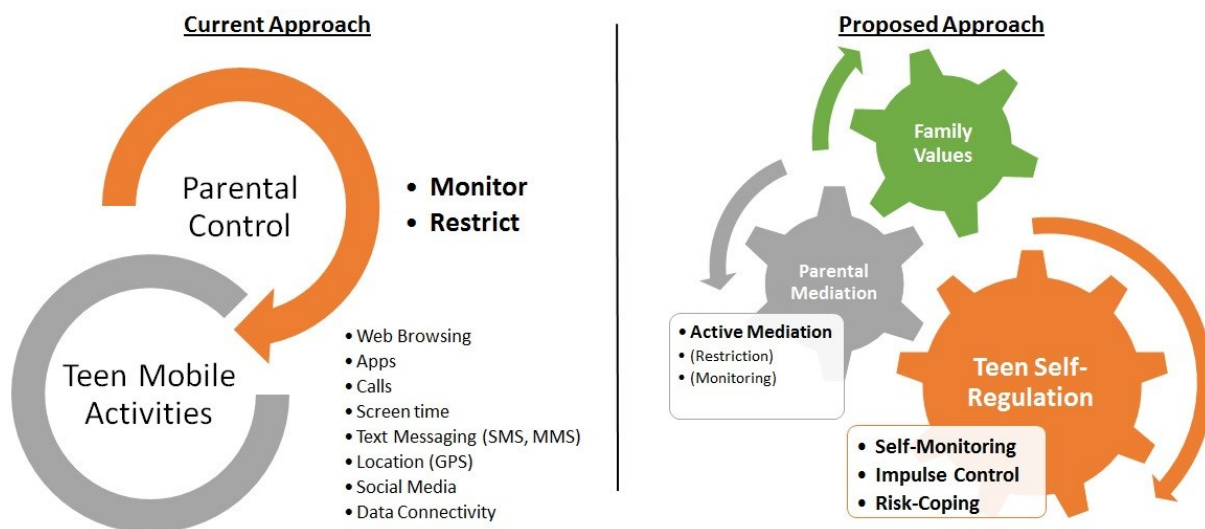


Figure 5: Current versus Proposed Approach for Teen Online Safety Apps

are potentially risky and, thus, in need of more awareness. Second, we need to study how to turn heightened awareness into better decision making processes.

Finally, we suggest app designs that more accurately acknowledge the shifting balance between parental control and teen autonomy as teens get older [8,9,49]. Apps for mobile online safety should arguably support *different* features depending on if the user is a child (under 12), young teen (13-15), or nearly an adult (16-17). However, we acknowledge that forcing the articulation of such awkward social tensions can in itself be a problem. A potential way to address this in future research would be to design more contingent rule-based systems that can adapt over time, and possibly even circumstance. For example, app information privacy rules can be implemented that evolve over time, or perhaps that evolve in response to stereotypical patterns of teens' online behavior.

Another approach would be to couch the problem as a *family systems* [17,61] challenge that the family works on collaboratively. The shifting control-autonomy balance could then be managed through appropriation - adopting roles and responsibilities through time and circumstances. Hiniker et al.'s work supports this approach as they found that more collaborative practices between parents and teens improve child buy-in, increase compliance, and more closely embody the value of fairness [31]. This is also a more active co-construction approach than the adaptive "rules" approach described above, but bears the same caution in that the actions embedded in the technology must be relatively lightweight and easily reversible, so as not to get in the way or supersede the underlying family developmental processes or values. The overall goal is to be more cognizant of the values in the design of mobile apps so that they reflect strategies that have been proven to support healthy adolescent development [8,55].

Limitations and Future Research

Our findings are constrained by a number of limitations. For instance, the feature analysis was performed on one mobile device. Therefore, some of the usability issues we encountered may not be generalizable to other devices. Otherwise, we made some methodological decisions when designing our study, such as restricting our analysis to apps that were freely available for download via the Android platform, that may also influence the generalizability of our findings. Below we will provide some rationale for these decisions and suggest ways that future research can build upon our results to further address these limitations.

We specifically chose to focus on the Android platform for a number of reasons: First, unlike Android's more open development platform, iOS developers are confined to a "sandbox" that prevents their apps from accessing key iOS phone functionality, such as text messages, screen time, and app controls [77], which we found to be integral components of the mobile online safety apps. As such, parental controls are natively built into Apple's iOS app

settings opposed to being offered more broadly through third-party apps. Second, we performed an initial app search in 2014 across the Apple App Store, Google Play, and the Microsoft App Store. Very few apps were identified on the Microsoft Windows platform, and we found a fairly large overlap (32%) in the apps available across the iOS and Android platforms. All platforms showed similar trends toward app features that promoted parental control through restriction and monitoring. However, by the time we began writing this paper, a number of the apps found in our initial search no longer existed, preventing us from completing our analysis. Thus, we chose to redo the app search and analysis in 2016, focusing only on Android apps. Given the relatively high overlap we found across the two platforms and Android's lion share of the market, we felt that this was a reasonable decision. Yet, we encourage future research to compare and contrast the Apple iOS implementation of mobile online safety for teens versus our results, which are more generalizable to the Google Android platform.

Overall, we are confident about the comprehensiveness of our search because we reached a saturation point such that all "suggested apps" had already been included in our sample. We also believe that our search was considerably more rigorous than how parents or teens would search for similar apps. Yet, our list of apps is only a representative sample, and not by any means, exhaustive. Our analysis was also constrained because we could not afford to pay for the premium versions of the apps. From reviewing the descriptions for the paid apps, we did not identify features that drastically shifted the nature of the apps, making them more supportive of parental active mediation or teen self-regulation. Future work could still extend our results by conducting a more in-depth feature analysis of paid apps.

Finally, in order to iteratively and fully integrate the principles of VSD [25,26] in the design of adolescent online safety apps, we recommend that researchers proceed in some of the following directions: First, our analysis was primarily a technical investigation [26] that identified app features that mapped to our conceptual TOSS framework. We did not directly engage with any of the key stakeholders in the mobile online safety space. It would be helpful, for instance, for researchers to interface directly with app designers to better understand their motivations, and subsequently, the values they implicitly or explicitly chose to embed in their apps. It is also imperative that future research include more user studies involving parents and teens. Engaging directly with users would provide invaluable insights into the values held dear by both individuals, and within families as a whole, helping researchers and designers identify which values are shared between parents and teens, which conflict, and, ultimately, areas where compromises can be made to serve both.

Only through a clear understanding of family values and tensions can designers begin to conceptualize technical approaches that may be viable solutions for mobile online safety or, in the very least, identify why technology-based

approaches may not be the best solution. The stakeholder and user studies suggested above align well with VSD's empirical approach [26] and would be worthwhile pursuits for future research. To these ends, we are currently in the early stages of partnering with a parental control app company to conduct usability tests with parents and teens using a beta version of their software.

CONCLUSION

We used the lens of value sensitive design [25] to reverse engineer the subset of family values embedded in the design of 75 mobile apps currently available to parents and teens for adolescent online safety. What we found was 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. Yet, what these values overlook is that teens are in the process of developing into young adults; therefore, need to learn how to cope with online challenges on their own [59,62]. This is reminiscent of boyd's work, which observes that, "as a society, we often spend so much time worrying about young people that we fail to account for how our paternalism and protectionism hinders teens' ability to become informed, thoughtful, and engaged adults" [14:28]. As such, we call for new design practices that are more teen-centric and place value on online safety as an integral part of their adolescent and developmental growth, teaching teens the confidence and skills to engage safely and smartly with others through mobile smart devices.

ACKNOWLEDGMENTS

We would like to thank the research assistants, Arun Kulshreshth, Rebecca Tsang, and Alan Totten, who initially helped code the data. Also, this research was partially supported by the U.S. National Science Foundation under grant CNS-1018302. Part of the work of Heng Xu was done while working at the U.S. National Science Foundation. Any opinion, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the U.S. National Science Foundation.

REFERENCES

1. Jonathan Ackley. 2007. Cell phone parental control. Retrieved May 22, 2016 from <http://www.google.com/patents/US7302272>
2. Giuseppe Amato, Paolo Bolettieri, Gabriele Costa, Francesco la Torre, and Fabio Martinelli. 2009. Detection of Images with Adult Content for Parental Control on Mobile Devices? *Proceedings of the 6th International Conference on Mobile Technology, Application & Systems*, ACM, 35:1–35:5. <http://doi.org/10.1145/1710035.1710070>
3. Morgan G. Ames, Janet Go, Joseph "Jofish" Kaye, and Mirjana Spasojevic. 2011. Understanding Technology Choices and Values Through Social Class. *Proceedings of the ACM 2011 Conference on Computer Supported Cooperative Work*, ACM, 55–64. <http://doi.org/10.1145/1958824.1958834>
4. Monica Anderson. 2016. Parents, Teens and Digital Monitoring. *Pew Research Center: Internet, Science & Tech*. Retrieved May 22, 2016 from <http://www.pewinternet.org/2016/01/07/parents-teens-and-digital-monitoring/>
5. Zahra Ashktorab and Jessica Vitak. 2016. Designing Cyberbullying Mitigation and Prevention Solutions Through Participatory Design With Teenagers. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, ACM, 3895–3905. <http://doi.org/10.1145/2858036.2858548>
6. Albert Bandura. 1991. Theories of Cognitive Self-Regulation. *Social cognitive theory of self-regulation. Organizational Behavior and Human Decision Processes* 50, 2: 248–287. [http://doi.org/10.1016/0749-5978\(91\)90022-L](http://doi.org/10.1016/0749-5978(91)90022-L)
7. Roy F. Baumeister and Todd F. Heatherton. 1996. Self-Regulation Failure: An Overview. *Psychological Inquiry* 7, 1: 1–15. http://doi.org/10.1207/s15327965pli0701_1
8. Diana Baumrind. 1987. A developmental perspective on adolescent risk taking in contemporary America. *New directions for child development*, 37: 93–125.
9. Diana Baumrind. 2005. Patterns of parental authority and adolescent autonomy. *New Directions for Child and Adolescent Development* 2005, 108: 61–69. <http://doi.org/10.1002/cd.128>
10. Antoine Bechara. 2005. Decision making, impulse control and loss of willpower to resist drugs: a neurocognitive perspective. *Nature Neuroscience* 8, 11: 1458–1463. <http://doi.org/10.1038/nm1584>
11. Samantha Biegler and danah boyd. 2010. behaviors and online safety: A 2010 literature review. Retrieved from <http://www.zephorias.org/files/2010SafetyLitReview.pdf>
12. Lindsay Blackwell, Emma Gardiner, and Sarita Schoenebeck. 2016. Managing Expectations: Technology Tensions Among Parents and Teens. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, ACM, 1390–1401. <http://doi.org/10.1145/2818048.2819928>
13. Ross Bott. 2013. Parental control of mobile content on a mobile device. Retrieved May 22, 2016 from <http://www.google.com/patents/US20130031601>
14. danah boyd. 2014. *It's Complicated: the social lives of networked teens*. Yale University Press.
15. Paul Carpenter and Allen East. 2007. Methods, devices, and computer program products for providing parental control over access to media content using a mobile terminal. Retrieved May 22, 2016 from <http://www.google.com/patents/US20070150918>

16. B.J. Casey, Rebecca M. Jones, and Todd A. Hare. 2008. The Adolescent Brain. *Annals of the New York Academy of Sciences* 1124, 1: 111–126. <http://doi.org/10.1196/annals.1440.010>
17. E. Mark Cummings, Kathleen N. Bergman, and Kelly A. Kuznicki. 2014. Emerging Methods for Studying Families as Systems. In *Emerging Methods in Family Research*, Susan M. McHale, Paul Amato and Alan Booth (eds.). Springer International Publishing, 95–108. Retrieved May 25, 2016 from http://link.springer.com/chapter/10.1007/978-3-319-01562-0_6
18. Alexei Czeskis, Ivayla Dermendjieva, Hussein Yapit, et al. 2010. Parenting from the pocket: value tensions and technical directions for secure and private parent-teen mobile safety. ACM Press, 1. <http://doi.org/10.1145/1837110.1837130>
19. L. D’Haenens, S. Vandonink, and V. Donoso. 2013. *How to cope and build resilience*. EU Kids Online. Retrieved from <http://eprints.lse.ac.uk/48115/1/How%20to%20cope%20and%20build%20online%20resilience%20%28lsero%29.pdf>
20. A. Duerager and S. Livingstone. 2012. *How can parents support children’s internet safety?* Retrieved from <http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/ParentalMediation.pdf>
21. M. Dumont & Provost, M. A. 1999. Resilience in adolescents: Protective role of social support, coping strategies, self-esteem, and social activities on experience of stress and depression. *Journal of youth and adolescence* 28, 3: 343–363.
22. Matthew S. Eastin, Bradley S. Greenberg, and Linda Hofschire. 2006. Parenting the Internet. *Journal of Communication* 56, 3: 486–504. <http://doi.org/10.1111/j.1460-2466.2006.00297.x>
23. Lee B. Erickson, Pamela Wisniewski, Heng Xu, John M. Carroll, Mary Beth Rosson, and Daniel F. Perkins. 2015. The boundaries between: Parental involvement in a teen’s online world. *Journal of the Association for Information Science and Technology*: n/a-n/a. <http://doi.org/10.1002/asi.23450>
24. 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.
25. Batya Friedman, Peter H. Kahn Jr, Alan Borning, and Alina Hultgren. 2013. Value Sensitive Design and Information Systems. In *Early engagement and new technologies: Opening up the laboratory*, Neelke Doorn, Daan Schuurbiens, Ibo van de 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
26. 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>
27. Batya Friedman, Peter H. Kahn, and Alan Borning. 2006. Value Sensitive Design and Information Systems. *Human-Computer Interaction and Management Information Systems: Foundations*. M.E. Sharpe, 348–372.
28. Gardner TW, Dishion TJ, and Connell AM. 2008. Adolescent self-regulation as resilience: resistance to antisocial behavior within the deviant peer context. *Journal of abnormal child psychology* 36, 2: 273–284.
29. Kilem L. Gwet. 2010. *Handbook of Inter-Rater Reliability, 4th Edition: The Definitive Guide to Measuring The Extent of Agreement Among Raters*. Advanced Analytics, LLC, Gaithersburg, MD.
30. Yasmeen Hashish, Andrea Bunt, and James E. Young. 2014. Involving Children in Content Control: A Collaborative and Education-oriented Content Filtering Approach. *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems*, ACM, 1797–1806. <http://doi.org/10.1145/2556288.2557128>
31. Alexis Hiniker, Sarita Y. Schoenebeck, and Julie A. Kientz. 2016. Not at the Dinner Table: Parents’ and Children’s Perspectives on Family Technology Rules. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, ACM, 1376–1389. <http://doi.org/10.1145/2818048.2819940>
32. ISTTF. 2008. *Enhancing Child Safety and Online Technologies*. Harvard University’s Berkman Center for Internet and Society. Retrieved from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf
33. Gill Jagger and Caroline Wright. 1999. *Changing Family Values*. Taylor & Francis.
34. Haiyan Jia, Pamela J. Wisniewski, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2015. Risk-taking As a Learning Process for Shaping Teen’s Online Information Privacy Behaviors. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*. ACM, 583–599. <http://doi.org/10.1145/2675133.2675287>
35. Lisa M. Jones, Kimberly J. Mitchell, and David Finkelhor. 2012. Trends in Youth Internet Victimization: Findings From Three Youth Internet Safety Surveys 2000–2010. *Journal of Adolescent Health* 50, 2: 179–186. <http://doi.org/10.1016/j.jadohealth.2011.09.015>
36. Atika Khurana, Amy Bleakley, Amy B. Jordan, and Daniel Romer. 2015. The protective effects of parental

- monitoring and internet restriction on adolescents' risk of online harassment. *Journal of Youth and Adolescence* 44, 5: 1039–1047. <http://doi.org/10.1007/s10964-014-0242-4>
37. Minsam Ko, Seungwoo Choi, Subin Yang, Joonwon Lee, and Uichin Lee. 2015. FamiLync: Facilitating Participatory Parental Mediation of Adolescents' Smartphone Use. *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, ACM, 867–878. <http://doi.org/10.1145/2750858.2804283>
 38. Claire B. Kopp. 1982. Antecedents of self-regulation: A developmental perspective. *Developmental Psychology* 18, 2: 199–214. <http://doi.org/10.1037/0012-1649.18.2.199>
 39. Richard S. Lazarus. 2000. Toward better research on stress and coping. *The American Psychologist* 55, 6: 665–673.
 40. Sook-Jung Lee and Young-Gil Chae. 2012. Balancing participation and risks in children's Internet use: the role of internet literacy and parental mediation. *Cyberpsychology, Behavior and Social Networking* 15, 5: 257–262. <http://doi.org/10.1089/cyber.2011.0552>
 41. Amanda Lenhart. 2015. Mobile Access Shifts Social Media Use and Other Online Activities. *Pew Research Center: Internet, Science & Tech*. Retrieved May 14, 2016 from <http://www.pewinternet.org/2015/04/09/mobile-access-shifts-social-media-use-and-other-online-activities/>
 42. 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/>
 43. Sonia Livingstone and Ellen J. Helsper. 2008. Parental Mediation of Children's Internet Use. *Journal of Broadcasting & Electronic Media* 52, 4: 581–599. <http://doi.org/10.1080/08838150802437396>
 44. Thomas Mazerski, Randy Moore, Joseph Taylor, Martin Gotlieb, and Marilyn Meyerson. 2006. System and method for secure web-based mobile phone parental controls. Retrieved May 22, 2016 from <http://www.google.com/patents/US20060293057>
 45. Gustavo S. Mesch. 2009. Parental Mediation, Online Activities, and Cyberbullying. *CyberPsychology & Behavior* 12, 4: 387–393.
 46. Kimberly Mitchell, Lisa Jones, David Finkelhor, and Janis Wolak. 2014. Trends in Unwanted Online Experiences and Sexting : Final Report. *Crimes Against Children Research Center*. Retrieved from <http://scholars.unh.edu/ccrc/49>
 47. Kristin L.1 Moilanen, Katie E.1 Rasmussen, and Laura M.2 Padilla-Walker. 2015. Bidirectional Associations Between Self-Regulation and Parenting Styles in Early Adolescence. *Journal of Research on Adolescence (Wiley-Blackwell)* 25, 2: 246–262. <http://doi.org/10.1111/jora.12125>
 48. S. Petronio. 2010. Communication privacy management theory: What do we know about family privacy regulation? *Journal of Family Theory & Review* 2, 3: 175–196.
 49. Sandra Petronio. 1994. Privacy binds in family interactions: The case of parental privacy invasion. In *The dark side of interpersonal communication*, W. R. Cupach B. H. Spitzberg (ed.). Lawrence Erlbaum Associates, Inc, Hillsdale, NJ, England, 241–257.
 50. Erika S. Poole and Tamara Peyton. 2013. Interaction Design Research with Adolescents: Methodological Challenges and Best Practices. *Proceedings of the 12th International Conference on Interaction Design and Children*, ACM, 211–217. <http://doi.org/10.1145/2485760.2485766>
 51. I. Seiffge-Krenke. 1995. *Stress, coping, and relationships in adolescence*. Lawrence Erlbaum, Mahwah, NJ.
 52. Wonsun Shin and Nurzali Ismail. 2014. Exploring the role of parents and peers in young adolescents' risk taking on social networking sites. *Cyberpsychology, Behavior and Social Networking* 17, 9: 578–583. <http://doi.org/10.1089/cyber.2014.0095>
 53. L. Steinberg. 2004. Risk taking in adolescence: what changes, and why? *Annals of the New York Academy of Sciences* 1021, 1: 51–58.
 54. L. Steinberg. 2008. A social neuroscience perspective on adolescent risk-taking. *Developmental review* 28, 1: 78–106.
 55. L. Steinberg, S. D. Lamborn, S. M. Dornbusch, and N. Darling. 1992. Impact of parenting practices on adolescent achievement: Authoritative parenting, school involvement, and encouragement to succeed. *Child Development* 63. <http://doi.org/10.2307/1131532>
 56. A.L. Strauss and J.M. Corbin. 1998. *Basics of qualitative research: techniques and procedures for developing grounded theory*. Sage Publications. Retrieved from <http://books.google.com/books?id=wTwyUnHYsmMC>
 57. Patti M. Valkenburg, Marina Krumar, Allerd L. Peeters, and Nies M. Marseille. 1999. Developing A Scale to Assess Three Styles of Television Mediation: “Instructive Mediation,” “Restrictive Mediation,” and “Social Coviewing.” *Journal of Broadcasting & Electronic Media* 43, 1: 52–66.
 58. Pamela J. Wisniewski, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2014. Adolescent Online Safety: The “Moral” of the Story. *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing*, ACM, 1258–1271. <http://doi.org/10.1145/2531602.2531696>
 59. Pamela Wisniewski, Haiyan Jia, Na Wang, et al. 2015. Resilience Mitigates the Negative Effects of Adolescent

- Internet Addiction and Online Risk Exposure. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ACM, 4029–4038. <http://doi.org/10.1145/2702123.2702240>
60. 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. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, ACM, 302–316. <http://doi.org/10.1145/2675133.2675293>
61. Pamela Wisniewski, Heng Xu, Jack Carroll, and Mary Beth Rosson. 2013. Grand Challenges of Researching Adolescent Online Safety: A Family Systems Approach. Retrieved May 25, 2016 from <http://aisel.aisnet.org/amcis2013/SocialTechnicalIssues/GeneralPresentations/10>
62. 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. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, ACM, 3919–3930. <http://doi.org/10.1145/2858036.2858317>
63. Sarita Yardi and Amy Bruckman. 2012. Income, Race, and Class: Exploring Socioeconomic Differences in Family Technology Use. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 3041–3050. <http://doi.org/10.1145/2207676.2208716>
64. Michele L. Ybarra, David Finkelhor, Kimberly J. Mitchell, and Janis Wolak. 2009. Associations between blocking, monitoring, and filtering software on the home computer and youth-reported unwanted exposure to sexual material online. *Child Abuse & Neglect* 33, 12: 857–869. <http://doi.org/10.1016/j.chiabu.2008.09.015>
65. 2014. Parents: A guide to Snapchat. *Webwise*. Retrieved July 23, 2016 from <http://www.webwise.ie/parents/parents-a-guide-to-snapchat/>
66. 2015. ReThink before the damage is done. Retrieved September 22, 2015 from <http://www.rethinkwords.com/>
67. Kik messaging app scrutinized in wake of Va. teen’s murder. *USA TODAY*. Retrieved May 26, 2016 from <http://www.usatoday.com/story/news/nation/2016/02/04/kik-messaging-app-scrutinized-wake-va-teens-murder/79826224/>
68. Campus uproar over Yik Yak app after sex harassment, murder - May. 7, 2015. Retrieved May 26, 2016 from <http://money.cnn.com/2015/05/07/technology/yik-yak-university-of-mary-washington/>
69. Parents Who Fight. *Facebook*. Retrieved May 26, 2016 from <https://www.facebook.com/ParentsWhoFight/>
70. Best Choice for Teens’ Cyber Safety – Parental Control App! Retrieved May 26, 2016 from <https://www.hackread.com/teens-cyber-safety-protection-parental-control-app/>
71. Using your Values to Raise your Children. *The Center for Parenting Education*. Retrieved May 27, 2016 from <http://centerforparentingeducation.org/library-of-articles/indulgence-values/values-matter-using-your-values-to-raise-caring-responsible-resilient-children-what-are-values/>
72. IDC: Smartphone OS Market Share. *www.idc.com*. Retrieved May 27, 2016 from <http://www.idc.com/prodserv/smartphone-os-market-share.jsp>
73. Nexus 5X. Retrieved July 19, 2016 from <https://www.google.com/nexus/5x/>
74. Marshmallow. Retrieved July 19, 2016 from <https://www.android.com/versions/marshmallow-6-0/>
75. *Child Safety Online*. Retrieved from <https://play.google.com/store/apps/details?id=com.ChildSafety.App>
76. TeenSafe Child - Android Apps on Google Play. Retrieved May 27, 2016 from <https://play.google.com/store/apps/details?id=com.systemcdms.com>
77. iOS vs Android. *Parent Tech Guide*. Retrieved July 19, 2016 from <http://parenttechguide.com/ios-vs-android/>

APPENDIX A

Table 5: Features and Strategies Matrix

Features*	Parental Strategy	Teen Strategy	Description and (<i>Codes</i>)	Cohen's κ (Parent)	Cohen's κ (Teen)
REPORTING	Monitoring	Self-Monitoring	Features that support sending reports to parents or teens regarding online activities (<i>No, Push, Pull</i>)	0.78	1.0
LOCATION-LOG	Monitoring	Self-Monitoring	Features track the physical location of the mobile device (<i>No, Details, Summary, Both</i>)	0.89	1.0
CONNECT-LOG	Monitoring	Self-Monitoring	Features that monitor data connections e.g., data, Wi-Fi, Bluetooth. (<i>No, Details, Summary, Both</i>)	1.0	1.0
CONNECT-BLOCK	Restriction	Impulse Control	Features that support blocking the data connection of the mobile device (<i>No, All, Some, Suggest</i>)	0.48**	1.0
KEYBOARD-LOG	Monitoring	Self-Monitoring	Features that track what is typed via the device's keyboard (<i>No, Details, Summary, Both</i>)	1.0	1.0
KEYBOARD-BLOCK	Restriction	Impulse Control	Features that actively regulate keyboard activity of the mobile device (<i>No, All, Some, Suggest</i>)	1.0	1.0
SCREENTIME-LOG	Monitoring	Self-Monitoring	Features that support the monitoring of screen-time activities (<i>No, Details, Summary, Both</i>)	1.0	1.0
SCREENTIME-BLOCK	Restriction	Impulse Control	Features that support the active regulation of screen-time activity (<i>No, All, Some, Suggest</i>)	1.0	1.0
CALL-LOG	Monitoring	Self-Monitoring	Features that support monitoring calls to and from the mobile device (<i>No, Details, Summary, Both</i>)	0.87	1.0
CALL-BLOCK	Restriction	Impulse Control	Features that actively regulate incoming and outgoing phone calls (<i>No, All, Some, Suggest</i>)	0.86	1.0
TXTMSG-LOG	Monitoring	Self-Monitoring	Features that support monitoring text messaging activity (<i>No, Details, Summary, Both</i>)	0.79	1.0
TXTMSG-BLOCK	Restriction	Impulse Control	Features that support the active regulation of text messaging activity (<i>No, All, Some, Suggest</i>)	0.74	1.0
BROWSER-LOG	Monitoring	Self-Monitoring	Features that support monitoring browsing activity (<i>No, Details, Summary, Both</i>)	0.71	1.0
BROWSER-BLOCK	Restriction	Impulse Control	Features that support actively regulating web browsing (<i>No, All, Some, Suggest</i>)	0.87	1.0
APP-LOG	Monitoring	Self-Monitoring	Features that support monitoring app activity (<i>No, Details, Summary, Both</i>)	0.73	1.0
APP-BLOCK	Restriction	Impulse Control	Features that support actively regulating app activities (<i>No, All, Some, Suggest</i>)	0.87	1.0
SOCMED-LOG	Monitoring	Self-Monitoring	Features that support monitoring social media activities (<i>No, Details, Summary, Both</i>)	0.72	1.0
SOCMED-BLOCK	Restriction	Impulse Control	Features that support actively regulating social media activities (<i>No, All, Some, Suggest</i>)	0.48**	1.0
SEEK-HELP-T	N/A	Risk-Coping	Features that support teens seeking help in the event of an emergency (e.g., "SOS") (<i>No, Yes</i>)	N/A	0.83
NEGOTIATE	Active Mediation	Risk-Coping	Features that support collaborative communication between parents and teens regarding the teens' online activities (<i>No, Yes</i>)	1.0	1.0
EDUCATE	Education	Education	Features that support educating parents or teens about online safety (<i>Yes, No</i>)	0.72	0.80

* The suffix "-T" was used to denote when a feature was available for teens. No suffix implies the feature was for parents only

**These IRR value are unusually low because there were only two codes (e.g., No/Some) applied to the data set and only one disagreement across the 15 apps. However, since the probability of random agreement for two codes is high and actual feature occurrence was low, it drastically reduced the overall IRR [29].

Table 6: Apps Included in the Feature Analysis (Last updated from Google Play on June 21, 2016)

App Name (URL)	Review (Out of 5)	# Reviews	# Installations	Date Updated
Accountability Soft	2.6	10	1,000 - 5,000	19-May-16
Alert.Us - Family Safety GPS	3.5	55	5,000 - 10,000	14-May-14
Anti Theft & Hacker Security	<i>No longer available on Google Play</i>			
bCyberwise Monster Family	4	47	1,000 - 5,000	23-Oct-13
Bitdefender Parental Control	2.9	663	50,000 - 100,000	19-Feb-16
Call & Message Tracker -Remote	4	2,406	100,000 - 500,000	11-Aug-14
Cerberus anti theft	4.4	89,982	1,000,000 - 5,000,000	15-Apr-16
Child Safety Online	2.5	4	1,000 - 5,000	31-Dec-12
Cybersafe	4.2	15	500 - 1,000	9-Jul-14
DigitalCitizen			100 - 500	3-Mar-15
Discovery Schools Trust	3	2	10 - 50	25-Sep-15
ESET Parental Control	3.5	877	50,000 - 100,000	23-May-16
Ever Accountable	4.6	395	10,000 - 50,000	30-May-16
Familoop Parental Control	4	147	5,000 - 10,000	5-Apr-16
FamilyTime - Parental Control	4.1	283	10,000 - 50,000	23-May-16
Funamo Accountability	3.7	190	10,000 - 50,000	13-Jun-16
Funamo Parental Control	3.3	1,167	100,000 - 500,000	13-Jun-16
G Student	3	2	100 - 500	27-Jan-16
Happy Onlife	4.4	21	500 - 1,000	1-Feb-16
Internet Safety	3.7	3	100 - 500	22-Jun-14
Kakatu (Parental Control)	4	1,157	100,000 - 500,000	16-May-16
KidnParent App (KnP)	3.1	64	1,000 - 5,000	5-Feb-15
KIDOZ: Discover the Best	4.1	15,408	1,000,000 - 5,000,000	29-May-16
KidRead : Parental control	3.5	196	10,000 - 50,000	22-May-14
Kids Place - Parental Control	3.9	14,741	1,000,000 - 5,000,000	17-Jun-16
Kids Zone Parental Controls	4	1,620	100,000 - 500,000	8-Jun-16
Kidslox FREE Parental Controls	3.7	105	1,000 - 5,000	19-May-16
KidzSearch Safe Web Browser	4.5	11	1,000 - 5,000	15-Feb-16
KuuKla Parental Control	3.5	147	10,000 - 50,000	29-Feb-16
MamaBear Family Safety	3.2	1,228	100,000 - 500,000	15-Feb-16
McAfee Family Protection	3.1	1,532	100,000 - 500,000	29-Sep-15
MMGuardian Parent App	4.3	1,422	50,000 - 100,000	7-Apr-16
Mobicip Monitor	3.8	14	1,000 - 5,000	21-Dec-15
Mobicip Safe Browser	3	1,005	50,000 - 100,000	31-May-16
Mobile Fence Parental Control	3.2	10,128	100,000 - 500,000	9-Jun-16
Mobile Phone Tracker	3.9	3,226	500,000 - 1,000,000	11-Jun-14
Net Nanny for Android	2.5	1,574	100,000 - 500,000	25-May-16
Norton Family parental control	2.9	7,349	500,000 - 1,000,000	3-May-16
NQ Family Guardian	3.9	1,465	100,000 - 500,000	23-Sep-15
Parent Control - Land of Kids	4.6	51	500 - 1,000	14-Jun-15

App Name (URL)	Review (Out of 5)	# Reviews	# Installations	Date Updated
Parental Control	3.6	2,036	100,000 - 500,000	17-Jan-16
Parental Control - KIDSBE	3.8	58	1,000 - 5,000	21-Jan-16
Parental Control Safe Family	3	236	10,000 - 50,000	25-Apr-16
Parental Control and Dashboard	3.8	246	10,000 - 50,000	22-Jan-15
Parental Control Board	3.3	294	10,000 - 50,000	20-Jun-16
Parental control by iNetClean	3.4	32	1,000 - 5,000	18-May-16
Parental Control Family Safety	3.9	23	5,000 - 10,000	9-Sep-15
Parental Control Launcher	4.2	212	10,000 - 50,000	28-Feb-16
Parental Control SecureKids	4	136	5,000 - 10,000	3-Jun-16
Parental control. Block all !	3.7	282	10,000 - 50,000	12-Oct-15
Parentsaround Parental Control	2.8	724	50,000 - 100,000	17-Jun-16
PhoneWatcher - Mobile Tracker	4.1	952	50,000 - 100,000	25-Nov-15
Privacy Camp	4.8	4	50 - 100	15-Jan-15
Qustodio Parental Control	3.6	8,058	100,000 - 500,000	14-Jun-16
Ranger Pro Safe Browser	3.2	110	10,000 - 50,000	18-Oct-13
Remote Control	3.7	548	10,000 - 50,000	2-Oct-15
ReThink - Stops Cyberbullying	4.5	266	10,000 - 50,000	6-Feb-16
Safe Browser - The Web Filter	3.5	4,149	500,000 - 1,000,000	2-Dec-13
Safe Browser Parental Control	3.4	934	100,000 - 500,000	9-Jun-16
Safe Browsing Parental Control	3.4	888	50,000 - 100,000	1-Apr-14
Safe Kids – Parental Control	3.5	62	5,000 - 10,000	16-Oct-15
SafeKiddo Parental Control	4	148	5,000 - 10,000	7-Jun-16
Screen Time Companion App	3.3	7,119	500,000 - 1,000,000	8-Jun-16
Screen Time Parental Control	4	8,233	100,000 - 500,000	17-Jun-16
SecureTeen Parental Control	3.4	5,613	100,000 - 500,000	11-Apr-16
Securkin	4.4	14	100 - 500	11-Jun-14
ShieldMyTeen Parental Control	3.5	1,077	100,000 - 500,000	12-Apr-16
SURFIE - KIDS	5	4	100 - 500	31-Jan-16
Surfie-Parent	5	4	100 - 500	31-Jan-16
TangTracker e-Safety App	4.8	43	1,000 - 5,000	20-Apr-15
TeenSafe Child	2.1	223	10,000 - 50,000	6-Oct-15
Trackidz (Parental Control)	4.3	110	1,000 - 5,000	28-May-16
Web Blocker *ROOT*	3.3	397	50,000 - 100,000	25-Jan-15
WOT Mobile Security	4.3	123	5,000 - 10,000	21-May-16
Xooloo Parental Control	2.6	529	50,000 - 100,000	25-Feb-15