Safety vs. Surveillance: What Children Have to Say about Mobile Apps for Parental Control

Arup Kumar Ghosh,
Karla Badillo-Urquiola
University of Central Florida
Orlando, FL USA
arupkumar.ghosh@ucf.edu,
kcurquiola10@knights.ucf.edu

Shion Guha
Marquette University
Milwaukee, WI USA
shion.guha@marquette.edu

Joseph J. LaViola Jr.,
Pamela J. Wisniewski
University of Central Florida
Orlando, FL USA
jjl@eecs.ucf.edu,
pamwis@ucf.edu

ABSTRACT

Mobile applications ("apps") developed to promote online safety for children are underutilized and rely heavily on parental control features that monitor and restrict their child's mobile activities. This asymmetry in parental surveillance initiates an interesting research question – how do children themselves feel about such parental control apps? We conducted a qualitative analysis of 736 reviews of 37 mobile online safety apps from Google Play that were publicly posted and written by children (ages 8-19). Our results indicate that child ratings were significantly lower than that of parents with 76% of the child reviews giving apps a single star. Children felt that the apps were overly restrictive and invasive of their personal privacy, negatively impacting their relationships with their parents. We relate these findings with HCI literature on mobile online safety, including broader literature around privacy and surveillance, and outline design opportunities for online safety apps.

Author Keywords

Adolescents; mobile online safety; parental control apps

ACM Classification Keywords

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

INTRODUCTION

Adolescent online safety within mobile contexts has become a salient and problematic issue for families, because: 1) mobile smart devices are the most prolific medium for communication, 2) these devices lend themselves to "near constant" access to the internet, and 3) this access is often unmediated by parents [7,9]. Teens generally have a strong sense of personal privacy when it comes to their mobile devices [11], making the negotiation process between parental control and teen autonomy difficult to manage [16]. As a result, parents are often unaware or underestimate the amount and types of social media apps their teens use [7], as well as the online interactions their teens experience, which may put them at risk [65]. Since parental mediation has been identified as a key protective factor against harm resulting from negative online experiences [39], unmediated access to the internet via personal mobile devices, may be the weakest link in ensuring the safety of teens online. Recent research suggests these concerns may also extend to younger children (under the age of 13) as children access the internet from mobile devices at increasingly younger ages [22].

According to a 2016 Pew Research study, parents use a wide array of strategies to monitor their teens' technology use, including 16% of parents who install parental control applications ("apps") on their teens' mobile devices to filter and block inappropriate online activities [1]. In 2017, Wisniewski et al. [63] conducted a review of commercially available parental control apps and concluded that these apps approached online safety in a very heavy-handed manner (through parental restriction and monitoring) that ignored teens' needs for privacy and autonomy. Yet, a limitation of this research was that it was conducted as purely a technical investigation of app features without providing any empirical evidence to confirm what teens (or younger children) actually thought about these apps. Therefore, the goal of our research is to build upon and triangulate Wisniewski et al.'s conclusions by examining the perceptions of children (including teens) who use (or parents who installed) parental control apps on their mobile devices. We pose the following research questions:

RQ1: *Do children generally like or dislike when parental control apps are installed on their mobile devices?*

RQ2: *What rationale do children provide for liking or disliking parental control apps?*

RQ3: *How can we take children's viewpoints into account when designing mobile technologies for their online safety?*

To answer these questions, we conducted a thematic content analysis of 736 online reviews publicly posted by children, who felt strongly enough to post their opinions about mobile parental control apps via the Google Play app store. To our knowledge, we are the first to use online

CHI 2018, April 21–26, 2018, Montreal, QC, Canada
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-5620-6/18/04…$15.00
https://doi.org/10.1145/3173574.3173698

reviews (or "found data") to capture children's unfiltered opinions about mobile online safety apps. In doing so, our paper makes the following unique contributions:

- We contribute knowledge to the broader domain of the privacy and surveillance literature by examining the tensions that arise due to the inherent power and information asymmetries that are created within parent-child relationships when parents install parental control apps on their children's mobile devices.
- We highlighted the otherwise unheard voices of more than 700 children to give them more agency and control regarding the design of future mobile online safety apps.
- We make design-specific recommendations to improve the acceptance and effectiveness of online safety apps using a "child-centric" assessment of users' needs.

BACKGROUND

Privacy, Social Surveillance, and Visibility

There is a rich body of work in SIGCHI around online privacy, surveillance, and visibility. While most of this work is not centered around parental monitoring of their children's online activities, they do provide relevant insights. For instance, the idea of networked privacy [42] has become a prominent area of research (i.e., privacy is not just about individual control or disclosure but can also depend on one's social network, especially on social media where content can be shared by one's friends). Many researchers have also drawn from Nissenbaum's theory of privacy as contextual integrity [44], i.e., privacy is a negotiation of information between two or more parties depending on certain norms, biases, assumptions, and culture. Communication Privacy Management theory has also been leveraged within the SIGCHI community to frame privacy as a boundary negotiation process, where individuals choose to make sensitive disclosures, which then become co-shared information with one's confidants [49]. Recently, networked privacy [42] has also been used to examine how visibility within social networks affects privacy decisions.

These privacy theories center around the notions of information disclosures and visibility. Visibility of our actions affects how we think about or make impressions about one another. In turn, our social connections and various audiences use visibility as a means to socially surveil us and form impressions [15,23]. In the case of children, this is especially true. Children are in the process of newly constructing their social identity online [40], as well as learning how to navigate complexities, such as when and how to make appropriate information disclosures while interacting with others in online spaces. Parental surveillance adds yet another layer of complexity, as children now have to make such decisions (and mistakes) under the watchful, and often judgmental [65], eyes of their parents. Yet, unlike the various privacy theories, which tend to assume that users' have some level of control over their disclosure decisions [44,49], children often do not have a choice in the matter. Especially in cases where parents opt to use technical monitoring on their children's mobile devices, sensitive information disclosures become compulsory [63]. This may create unique tensions between parents and children as there are explicit trade-offs between the child's (especially for teens) digital privacy needs and their online safety [11,16].

Families and Mediating Technology Use in the Home

The majority of empirical research in the field of online safety relies heavily on survey-based parent and child self-reports around the child's online risk experiences and the factors that contribute to the likelihood of increased risk exposure [50]. Researchers from the SIGCHI community [7,11,28], have studied families and technology use more holistically; for instance, Blackwell et al. [7] studied the tensions that exist between parents and children around technology use in the home. They found that parents underestimate teens' social media use, teens' sometimes felt like their parents ignored their requests for privacy, and family rules around technology use were often broken by both parents and children. In contrast, Cranor et al. [11] found that parents agreed that teens need some degree of privacy, so that they can gain independence in online spaces. Meanwhile, Hiniker et al. [28] found that parental rules that constrain technology use (e.g., banning Snapchat), as opposed to context of use (e.g., "no phone at the dinner table,") were less likely to be broken. A common theme among these studies was the focus on the broader context of technology use in home settings and the tensions between parents and children around rule-setting to manage expectations and boundaries. None of the aforementioned studies specifically examined children's perceptions of having online safety apps installed on their smartphones.

Mobile Phones as a Tool for Parental Surveillance

Giving children cell phones can provide parents a means to monitor their child's physical whereabouts and serve as a "transitional object" as teens begin to separate from their parents [10,52,61]. Yet, those who have examined parental monitoring and parent-child perceptions of risk (in offline contexts) have found that surveillance and tracking may not be the most effective solution, as it may perpetuate paranoia and fear on the part of both parents and children [47,56]. For instance, Boesen et al. examined mobile-based location tracking and found that such tracking devices had the potential to undermine trust [8]. This has also been examined (with similar findings) by social computing researchers in at-home settings between family members [46,58]. Yet, less is known about how privacy boundaries are affected when mobile devices are used to explicitly monitor children's online activities via their mobile devices.

A More "Child-Centric" Approach to Online Safety

The central argument of our work is that children, particularly teens, should play a pivotal role in the design and development of the mobile apps that are designed to keep them safe. According to Poole and Peyton [51], "as a population, adolescents are understudied, poorly understood, and weakly represented in interaction design research" (p. 216). Involving adolescents in research is a challenging task, which has historically resulted in fewer studies that devote their time to working directly with teens [51], especially in the realm of online safety [50]. In 2009, Rode et al. [53] motivated their ethnographic study of 27 children and their security practices in the home based on the fact that children are often overlooked or marginalized within the HCI literature. Fortunately, researchers have begun to recognize the benefits of finding novel ways to involve children in the design phase for developing effective and interactive technologies to solve problems relevant to them, such as using participatory design approaches with teens to address cyberbullying [2]. Similarly, an over-arching theme within Wisniewski et al.'s research on adolescent online safety [63,64,66,67] has been to challenge others to take a more "teen-centric" and "resilience-based" approach. Such work has led to a paradigm shift away from more risk-adverse approaches of shielding teens from online risks to strength-based approaches for helping teens thrive in spite of the online risks they might encounter [34,64,67]. Our work adds to a growing body of literature that aims to give children a voice in the design of technologies that not only protect them, but may also directly benefit them.

FRAMEWORK OF TEEN ONLINE SAFETY STRATEGIES

Wisniewski et al.'s [63] work, which examined the features offered in existing mobile online safety apps, most closely motivates our current work. They created a theoretically-derived Teen Online Safety Strategies (TOSS) framework [63], which was used to illustrate the imbalance between strategies that support parental control versus teen self-regulation. The TOSS framework included three ***parental control strategies***: 1) *monitoring,* passive surveillance, 2) *restriction*, rules and limits regarding use, and 3) *active mediation*, communicating with one's teen. The three ***teen-self regulation strategies*** included: 1) *self-monitoring,* awareness of one's own actions, 2) *impulse control*, managing short-term desires to avoid long-term consequences, and 3) *risk-coping*, dealing with risky online interactions once they occur [63]. In this prior work, the researchers illustrated a striking imbalance in features that supported parental control (89%) over teen self-regulation (11%) and, from a technical standpoint, showed how teens seemed to be ignored in the design of these mobile apps. In the next section, we explain how the TOSS framework served as a theoretical lens for our qualitative analysis.

METHODS

Data Collection

Analyzing user reviews is a common practice for understanding users' opinions [19,54], though it has not been used in the context of apps for online safety**.** Therefore, we scraped publicly available user reviews based on Wisniewski et al.'s [63] list of 75 adolescent online safety apps available on Google Play. In August 2016, we used a program called Heedzy [70] to download the Google Play reviews into a comma delimited file. Each review had the following attributes: 1) app name, 2) date, 3) user name, 4) review, and 5) rating. Ratings were numerical values (represented as a "star") given by the user, ranging from 1 = worst to 5 = best. Our study did not require an IRB protocol because all reviews were publicly available, and we did not interact with any human subjects during data collection. A total of 29,272 user reviews for 66 apps were scraped. The app count went from 75 to 66 because a number of the apps from the previous work were no longer available.

Early on, we weighed the strengths versus the weaknesses of relying on online reviews to inform our research. The weaknesses of this approach include concerns that online reviews are bimodal, represent extreme viewpoints [32], and can be manipulated [30]. Yet, others have found the strengths of online reviews to be that they are helpful [37], dependable [3,31], and a useful, unobtrusive technique to inform product development [33]. Ratings and reviews add value to both app developers and potential new users by providing a crowd-sourced indication of app quality [59]. Online user reviews can also provide valuable insights that impact product sales [14]. We concluded that because qualitative and interpretive inquiry focuses on themes that emerge and converge across multiple informants, often embracing potential "outliers" [21], the benefits of being able to collect such a large sample of relevant feedback from actual teen app users, outweighed the limitations of using review data. Further, since we are triangulating Wisniewski et al.'s [63] findings from their feature analysis of these apps, this allows us to ground our work in their previous results. Therefore, in light of the novelty of our approach and these considerations, we proceeded with our in-depth qualitative analysis that uncovered latent stories underlying these reviews.

Data Analysis Approach

Upon initial analysis of the 29,272 scraped reviews, we determined that it was relatively easy to distinguish between teen reviews versus parental reviews. For example, teens often used phrases like "my parents," while parents would use phrases such as "my daughter." An example of a parent review is shown below:

> *"This app is great. The tasks help make it easy to keep* ***my daughter*** *on task. And that I can see where she's been online is great things."* –Five Star, Screen Time Parental Control, 2015

Since Google Play reviews are made by a single user account in which an app is installed, this implies that the scraped reviews were most likely mutually exclusive – either written by parents or children. With only a few hours of targeted key word searching (e.g., "my parents," "my mom," "my dad," "my father," "I am * old," "years old," and "my step") we found over 450 reviews posted by children. The first author then went through all 29K reviews manually to identify those made from the vantage point of a child. An undergraduate research assistant went through the entire data set again to find any other reviews that may have been missed. Our final data set includes 736 child reviews for 37 apps. Of the 66 apps, 29 apps did not appear to have any reviews written by children. Upon further examination, these apps either were not primarily used for child online safety (e.g., pornography addiction apps, anti-theft apps) or had a low number of total reviews.

Next, we conducted a thematic content analysis [17] to characterize the rationale for why teens liked or disliked the apps they reviewed. We leveraged a hybrid approach of template coding [17] based on theory (i.e., Wisniewski et al.'s TOSS framework [63]) and open-coding to allow flexibility for new themes to emerge. First, we coded the data based on the TOSS framework, which was derived from theoretical underpinnings from developmental psychology on the different approaches to promoting adolescent online safety [63]. However, we somewhat adjusted the lens by which we applied the TOSS framework; first, we coded child reviews based on whether they mentioned the six online safety strategies in some capacity but without regard to whether they liked the strategy or not. Second, we noted whether the use of such strategy was viewed positively or negatively.

Finally, we used a grounded, thematic approach [68] to identify other themes that were present in the reviews but not represented by the TOSS codes. The first author and research assistant independently coded all teen reviews with the lens of trying to understand the underlying rationale behind why teens liked or disliked the parental control apps. Then, the two coders met to discuss, form a consensus, and merge their codes. Axial coding [57] was used to align sub-themes into over-arching themes. The first author made a final pass through all of the child reviews to make sure that all codes had been applied consistently across the data set. We allowed multiple codes to apply to each review and double-counted in these instances. **Table 1** summarizes our final codebook, including the pre-defined codes from the TOSS framework (in bold), as well as twenty-four additional codes that emerged and were grouped under the seven main themes presented in this paper. Percentages represent the frequency in which each theme emerged.

	Main Themes	**Codes***
Disliked Apps (79%)	Overly Restrictive **(35%)**	**restriction**, rebellion, blocking, lack of freedom, oppressive, and anger
	Privacy Invasive **(23%)**	**monitoring**, privacy, stalking, and lack of respect
	Bad Parenting/ Lack of Communication **(14%)**	**active mediation**, upfront, communication, and lazy
	Faulty Design and Usability Issues **(14%)**	usability, design flaws, performance, and bugs
Liked Apps (21%)	Control Unhealthy Behaviors **(23%)**	**impulse control**, productivity, time management, addiction, and self-motivation
	Kept them Safe **(17%)**	**risk-coping**, peace of mind, and siblings/others
	Ability to Negotiate and More Freedom **(12%)**	**active mediation**, **self-monitoring**, good communication, negotiation, and freedom

* *Template codes based on the TOSS framework are shown in* **bold.**

Table 1. Final Codebook

We found that most reviews were written quite dichotomously – children either liked some aspect of the apps (not really loved) or disliked (pretty much hated) the apps. Even though a single review could reflect both positive and negative sentiments about the app during the coding process, we found that the ambivalence expressed in a minority of reviews was not relevant for discussion. Therefore, to facilitate the presentation of our results, we decided to split the reviews based on their star ratings (past research [29] also confers that the content of the reviews are often highly correlated with their star ratings). We considered a review with a rating with less than or equal to 2 stars as a low-rated review, and a rating of 3 or more stars as a high-rated review. We identified 581 low-rated reviews (i.e., "Disliked") and 155 high-rated reviews (i.e., "Liked").

RESULTS

Sample Characteristics

Reviews were posted between 2012 and 2016 given the following distribution: 2012 (<1%); 2013 (3%); 2014 (22%); 2015 (39%); and 2016 (36%). We observed ten instances where a child (based on username) left a review for multiple apps, and six reviews were left anonymously as, "A Google User," suggesting our analyses incorporates the opinions of at least 700 different child users ranging in age from 8 to 19. We found that some apps had a larger representation of child reviews than others. Screen Time Companion App had a total of 216 reviews, which represented 29% of the entire data set. Qustodio Parental Control and Mobile Fence Parental Control each had 80 reviews, representing another 22% of the data set. Generally, we saw a pattern where apps that had more child reviews typically had more downloads and total reviews overall. These apps, therefore, might have a larger user-base than some of the apps that had fewer child reviews.

Star ratings presented with the following distribution: 1 star (76%); 2 stars (3%); 3 stars (4%); 4 stars (3%); and 5 stars (14%). We found that the majority (79%) of children overwhelmingly disliked these apps, while a small minority (21%) of child reviews saw benefits to the apps. This is interesting and is an interpretive confirmation that online reviews are bimodal and come from extreme viewpoints [19]. We also compared the mean and standard deviation of child reviews (*M*=1.79; *SD*=1.48) to the remainder of the data set (N=28,536) reviews that were presumably made by parents (*M*=3.66; *SD*=1.79). Children rated the apps significantly lower than parents (mean difference between parents mean score was 1.866 (95% CI, 1.76 to 1.98) higher than children's mean score, $t(793.34) = 33.77$, $p < 0.05$).

Below, we present our results as children's rationale for disliking or liking mobile online safety apps. Illustrative quotes indicate the star rating as well as the app which was reviewed by each child. However, to maintain the confidentiality of the child users who posted reviews, we excluded user names and any other personally identifiable information when quoting from our data set.

Why Teens Disliked Apps

Approximately 79% (N=581) of the reviews were classified as low-rated. We analyzed these low-rated reviews and identified three emerging themes for why children in our study did not like these apps; we discuss each theme and sub-themes that emerged from our data below.

Children Found the Apps Overly Restrictive

Thirty-five percent of the reviews expressed that children thought that the apps were overly restrictive. However, 28% of these reviews didn't mention specific features were being blocked. Instead, children focused on the unwanted oppression itself and how such restrictions would lead them and other children to rebel against their parents:

"This app sucks. It has to much restriction. Parents if you really want your kids to hide more things from you and be more rebellious then get them to down load this app. Because they will become more defiant the more you restrict them and they will make your life a living hell because your overprotective." –One Star, Mobile Fence Parental Control, 2015

Many reviews suggested that the apps were so restrictive that the children could no longer accomplish everyday tasks, such as doing their homework:

"This app blocks just about everything! I'm a kid and I cant go on anything, not even my homework website." –One Star, Norton Family parental control, 2014

Children often complained that they could no longer use their phones for their intended purposes, so they were frustrated with their parents:

"My mom put this on my phone and now i cant do anything so why should i even have a phone." –One Star, Kids Place - Parental Control, 2014

They equated the high level of restriction to a lack of personal freedom. They felt that it was ironic that their parents would give them a personal digital device then limit the capabilities of what it was supposed to do:

"I don't even know why they make this kind of stuff! If a kid is old enough to have a phone or tablet, they are old enough to have FREEDOM." –One Star, Qustodio Parental Control, 2015

We noted the types of mobile activities children said were being restricted, and in 21% of the reviews, screen time restrictions were the most common. Children hated the time limits parents enforced on their phones and were frustrated at the negative impact of these restrictions, such as hampering their social lives:

"This is the worst app ever I can't even spend 2 hours on my phone today I am only allowed to go on my phone 1 time a day for only an hour I mean I am 15 I I have a life I have friends I have things to do and my friends with think I've deserted them." –One Star, Screen Time Companion App, 2016

Interestingly, we did not find any reviews where children were upset because the apps restricted them from inappropriate behaviors (e.g., watching porn). Instead, they considered the apps being "ridiculously" overly restrictive:

"It doesn't just protect you from the porn and stuff, it protects you from the whole internet!! It wouldn't let me look up puppies!...If I can give it less than a star I would!!" –One Star, Net Nanny for Android, 2014

Children who used words such as "restrict," "block," or "limit" in their reviews often used strong language, such as "hate," "horrible," "dumb," "bad," and "sucks." In short, children did not simply dislike the apps that they thought were overly restrictive; they despised them.

Teens Felt the Apps Were Invasive of Their Privacy

In another 23% of the low-rated reviews, children thought that the online safety apps violated their personal privacy and equated the apps to a form of parental stalking:

"This totally takes ALL my privacy away. I can't even talk to my biological dad, or my boyfriend, or best friend with out being stalked by my mom." –One Star, SecureTeen Parental Control, 2015

They brought up how they felt that the apps that monitored their every move negatively impacted the trust relationship they had with their parents:

"This app will cause trust issues with your kids. Ever since my dad installed this app, he and I have grown farther apart. If he doesn't trust me enough to use my phone, then why should I trust him?" –One Star, SecureTeen Parental Control, 2015

Others alluded to parents not giving them mutual respect by disregarding their privacy and insinuated that parents would not like if they were being treated with the same level of disregard:

"My mom put this on my phone. Awful invasion of privacy! Worst thing ever! Parents should be ashamed of themselves

for downloading this app because you are invading the private lives. Will be putting this on my mom's phone and seeing what happens! This is evil!" –One Star, SecureTeen Parental Control, 2014

Based on the reviews related to parental monitoring, children were annoyed that the apps tracked their "each and every move," ranging from their call logs, SMS messages, to social media activities.

Why Not Just Talk to Us?

In about 14% of the reviews, children were very vocal in their opinions about the apps not aligning with good parenting techniques, such as communicating with them or trusting them to make good decisions:

"Seriously, if you love your kids at all, why don't you try communicating with them instead of buying spyware. What's wrong with you all? And you say we're the generation with communication problems." –One Star, SecureTeen Parental Control, 2016

Others pointed out that they would rather their parents just be upfront with them and ask to see their phones. Monitoring and restricting their mobile activities through an app was disrespectful:

"Fantastic. Now now my mom is stalking me. I have nothing to hide. You can always just ask to go through my phone. Too invasive and down right disrespectful. Thanks for the trust, mom." –One Star, MamaBear Family Safety, 2014

Some teens pointed out that their parents were trying to use apps designed to monitor and restrict the mobile activities of younger children. They often felt it was inappropriate to use such apps for teens, and it was a "lazy" way to parent:

"This is a app for little kids like 10 or younger, I am 15 and my mom still put this on my phone. Parents should monitor there kids phones but I feel this app is to restrictive. So parents, don't take the lazy way out of parenting your kids, give them a chance with there phones. This really is a lazy parenting method of monitoring your child." –One Star, Screen Time Companion App, 2016

These teens felt that these apps were a poor way for parents to try to regulate the mobile activities of teens, as opposed to talking with them, trusting them, and taking more active approaches to parenting.

Faulty Design and Implementation of Apps

One final theme emerged from the data for why children did not like the apps. Fourteen percent of children commented on design flaws and performance issues of the apps. Performance issues included slow operation, difficulty using the app, bad battery life, and glitches:

"If I could this app I would give it a -5 starts this is a piace of poop it messes up my phone and it is more of a pain in the butt this need to be fixed of all its glitches." –One Star, NQ Family Guardian, 2014

Other children were frustrated that the apps did not work as they were supposed to, even for their parents:

"It's difficult to use. It doesn't work the way it's supposed to at all…My father has had to go through many hours of trying get this application to work correctly." –One Star, Net Nanny for Android, 2016

Some children disliked the apps but enjoyed their design flaws, which let them remove the apps from their phones:

"I'm,15 years old and I was not ok with this app and just like all the other crap they throw at me I bypass I bypassed this app in less then 5 minutes y'all need to do better." – One Star, Screen Time Parental Control, 2016

In summary, children in our study generally did not like the apps when they malfunctioned; yet, they also did not like the apps when they served their intended purposes.

Why Children Liked Apps

Only 21% (N=155) of the reviews were classified as high-rated and were grouped in three emerging themes below.

The Apps Helped Children Control Unhealthy Behaviors

Of the high-rated reviews, 23% of the reviews expressed appreciation that the app helped the children better manage their time, control unhealthy behaviors, and become more productive. For example, reviews talked about how these apps helped them control inappropriate impulses, such as being on their phones way too much:

"Me and my parents understood I needed this app. I was out of control but now with screentime I'm back on level ground." –Five Star, Screen Time Companion App, 2014

Some teens also realized the benefits of apps that helped them better manage their time and do better in school:

"I'm a teenager and I was glued to my phone but this app helped me manage myself very well! So thanks, your app improved my math grade!!!!"–Five Star, Screen Time Companion App, 2014

Others wanted to break unhealthy behaviors, such as addictions to pornography:

"I have a porn addiction and this app has saved my life." – Five Star, Mobile Fence Parental Control, 2016

Some children admitted they still found ways to look at porn, but they reduced the behavior because they wanted to earn their parents' trust:

"My parents put this on my phone…to protect me from porn. I have found ways around it but I don't use them because I want my parents to trust me." –Four Stars, Screen Time Companion App, 2016

Other children might not have originally liked the idea of an app that limited their screen time, but in the end, they respected their parents' decision because they realized that other things were more important:

“I'm a 14 year old girl. Yes, I like to keep up to date with social media and all of that but I do respect the decision of parents to use this app because it is bad for the eyes and brain to have you face stuck into an iPad all day and I'm no fully mature adult or a mother but it would be a good lesson to teach your child(ren) to enjoy whats around them such as sunny days, friends and family that they have now. I'm getting this app to use on myself so I am not head and eyes into things that are unimportant.” –Three Star, Screen Time Companion App, 2014

Some teens even opted to install apps themselves to help them regulate their own unhealthy mobile behaviors:

“I am a 19 and I'm using it for myself . Thanks a lot :) .” –Five Star, ShieldMyTeen Parental Control, 2016

“Im getting this for myself im 13 I need it bad I am on lots and I hate myself because of it. And if the creater can make an internet seach blocker that would also be good for me.” –Five Star, Screen Time Companion App, 2014

Many of these positive reviews were for Screen Time Companion, which had the largest representation in our data set. Teens who liked this app tended to agree that they had a problem disconnecting from their phones and liked that the app helped them to do so.

The Apps Helped Keep Children Safe

In about 17% of reviews, children talked about how apps made them feel safer. For instance, some teens had a peace of mind because their parents were watching over them:

“My dad has a way. Where he can see everything I post on social media and more to keep me safe thanks mama bear” –Five Star, MamaBear Family Safety, 2014

Other children talked about SOS emergency features that allowed them to contact their parent for help:

“If my mom is not at the bus stop I can hit panic and she can come to get me.” –Five Star, NQ Family Guardian, 2014

Some children used the apps to protect their mobile devices (and their privacy) from their siblings:

“I love this app! it keeps my sisters from going on things I don't want them to and buying things that will come off of my moms credit card.” –Five Star, Kids Place - Parental Control, 2014

While infrequent, some children saw some protective benefits of the apps, even if they were to protect their privacy from the prying eyes of others or to notify parents when the child needed assistance.

Children Could Negotiate with Parents for More Freedom

Another 12% of the positive reviews mentioned that apps helped children communicate or negotiate with their parents for more freedom with their mobile devices:

“Of course I'd rather not have it, but the flexible features makes it easy to negotiate with your parents.” –Three Star, Mobile Fence Parental Control, 2015

Children appreciated the reward system that some apps offered. Using this system, parents were able to provide positive reinforcement for their children via the app:

“My dad installed this onto my phone, now I'm on track more! I also love the reward time system, really creative!” –Five Stars, Screen Time Companion App, 2016

In some cases, children felt that they actually had more freedom to use their device because, otherwise, their parents would always be looking over their shoulders:

“Without this app, I wouldn't be allowed to have a tablet. I can do pretty much what I want, my parents aren't always looking over my shoulder.” –Five Stars, Funamo Parental Control, 2015

Children who liked the apps seemed to feel that the app either helped get their parents off of their backs, provided a reward system for positive behaviors, or at least let them negotiate limits set by the apps with their parents.

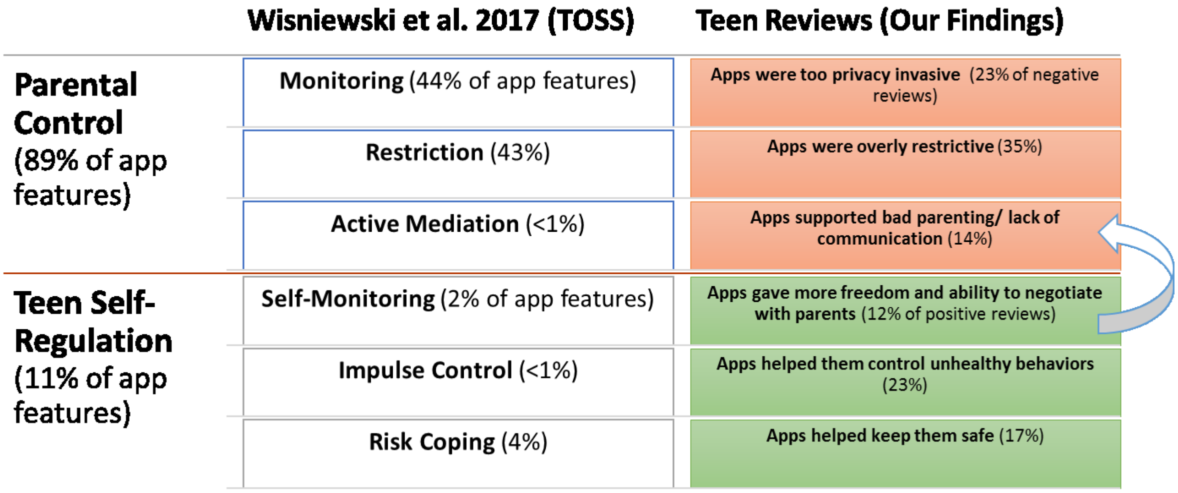
DISCUSSION

We discuss the theoretical and practical implications of our results, as well as make design-specific recommendations for future mobile online safety apps.

Triangulating Wisniewski et al.’s Findings

The unique contribution of our work, compared to Wisniewski et al.’s [63], is that their earlier research worked to understand what features embedded within the apps supported teen online safety, while we work towards understanding whether these features actually meet the needs of child users. In our analysis, children rarely mentioned specific features (unless they were discussing usability issues) of the respective apps; instead, they referenced the positive and (mostly) negative consequences that the apps had on their lives. Therefore, without the TOSS framework, we would have been unable able to triangulate our findings with Wisniewski et al.’s feature analysis because reviews and features were not one-to-one.

Yet, comparing our results through the TOSS framework (As shown in **Figure 1**), the reasons why children disliked apps aligned directly with the TOSS dimensions for parental control [63]; these were the online safety strategies that Wisniewski et al. [63] found were well-supported in the feature sets of the existing apps. In contrast, the reasons why children liked the apps aligned directly with the TOSS strategies that supported self-regulation, which Wisniewski et al. found to be woefully unsupported in the existing apps. Children saw the apps as overly restrictive (i.e., *parental restriction*) or invasive of their personal privacy (i.e., *parental monitoring*) instead of promoting features that directly benefitted them.



	Wisniewski et al. 2017 (TOSS)	Teen Reviews (Our Findings)
Parental Control (89% of app features)	**Monitoring** (44% of app features)	**Apps were too privacy invasive** (23% of negative reviews)
	Restriction (43%)	**Apps were overly restrictive** (35%)
	Active Mediation (<1%)	**Apps supported bad parenting/ lack of communication** (14%)
Teen Self-Regulation (11% of app features)	**Self-Monitoring** (2% of app features)	**Apps gave more freedom and ability to negotiate with parents** (12% of positive reviews)
	Impulse Control (<1%)	**Apps helped them control unhealthy behaviors** (23%)
	Risk Coping (4%)	**Apps helped keep them safe** (17%)

Figure 1. Triangulating Wisniewski et al.'s (2017) results through the TOSS Framework.

We found that child reviews were more positive when they felt that the apps afforded them more agency (i.e., *self-regulation*) or improved their relationship with their parents (i.e., *active mediation*). For instance, some children found apps useful when they helped them control unhealthy or addictive behaviors (i.e., *impulse control*) or gave them more awareness of their unhealthy behaviors (i.e., *self-monitoring*). Children were open to using online safety apps when they saw direct benefits, such as managing unhealthy behaviors. Further, we uncovered an interplay between self-monitoring and parental active mediation (as illustrated by the arrow in **Figure 1**) that suggests that when children are given the room to be more self-aware, this allowed them to have more agency in negotiating rules set by their parents for online safety regulation. Thus, our results indicate *why*, from a child's perspective, it is important to strike a better balance between parental control and self-regulation.

Asymmetries in Parental Control App Design

As we stated earlier, children are in the process of understanding and creating their own personal identities online [40]. Our research empirically illustrates how this process is further complicated when parents create asymmetric power differentials that attempt to control and monitor their children's online behaviors, especially for teens. On one hand, parents have a legal, ethical and moral obligation to manage the safety of their children; on the other hand, teens are making developmentally appropriate strides to separate themselves from their parents' authority over their lives [5,6]. This tension is implied (but not specifically addressed) in current and prevalent models of networked privacy [42]. There has been some recent work [18,24] on understanding what symmetric visibility means for perception of impressions and surveillance in social networks but none that specifically looks at the complex dynamics between parents and children. Communication studies have also examined the effects of parental privacy invasions in offline contexts [35], and our work further carves out a space to examine these privacy tensions within mobile and online contexts.

Children who posted reviews disliked when apps were overly restrictive, privacy invasive, took away their autonomy, and negatively impacted their relationship with their parents, showing they valued open communication and a trust-based relationship with their parents. We found that most children strongly disliked mobile online safety apps and seemed to be forced to use them by their parents who installed the apps on their mobile devices. Ultimately, they resented the *asymmetry* created by parental control apps, which was reflected in their reviews. A lot of discussion around the interrelated themes of online privacy, surveillance and visibility centers around the notion of asymmetry in visibility and in information access [9,25,41].

Thus, it is no surprise to us that the majority of child reviews were negative and focused on the forcefulness of their parents in imposing parental control apps on them. This is because these apps created a discernable imbalance, in terms of information and power, violating their contextual integrity [44] (as their information was being intercepted by unintended audiences, i.e., their parents) and exerting too much control over their online lives. The apps were less equipped to support parental active mediation or empower children in any meaningful way. Hence, the currently available parental control apps may undermine trust and harm children's relationship with their parents, and thus, are not the ideal solution for protecting them, at least in their present form. Instead, non-techno-centric approaches [4] that do not rely on technology could be used as a solution and, instead, promote face-to-face interactions between parents and children. With this in mind, we provide a number of online safety design recommendations that may work toward rectifying some of these issues.

Implications for Design

Many of the recommendations below are specific to teens, as opposed to younger children, due to their differing developmental needs for autonomy. Additionally, regulations, such as COPPA [69], provide legal safeguards for children under the age of 13 that discourage independent use of online services, such as social media, without parental supervision. As such, some of these recommendations may not be legally appropriate for younger children. However, our analysis suggests that children share many of the same concerns as teens regarding the restrictiveness and privacy invasiveness of parental control apps. Therefore, more research should be conducted to determine whether the recommendations below may also be useful for younger children.

Designing for Safety with Privacy in Mind

While the mobile apps analyzed provide a more transparent window into children's lives to calm the fear of parents, this transparency also seemed to come at a cost. During adolescence, teens need more personal and psychological space for positive development; privacy also becomes very important in terms of the parent-teen relationship in order to build trust and allow teens a level of personal autonomy [16,48]. A recent study [26] reveals that too much restriction or monitoring could hamper parent-teen trust relationship. Yet, Blackwell et al. [7] found that the "practical obscurity" (i.e., how information can be hidden from others) of children's mobile devices also creates anxiety for parents and encourages them to use more restrictive parenting strategies. In such situations, technology should help parents and teens (who have intergenerational differences) negotiate freedoms teens have online, which would help parents better manage their teens' mobile use and reduce tensions between parents and teens [27,36].

To compromise on a solution that may meet both parents' desire to keep their children safe and teens' desire to uphold personal privacy, we recommend that app designers create online safety apps that employ a level of abstraction [20] to give parents helpful meta-level information regarding teens' mobile activities instead of full disclosure of what teens do from their mobile phones similar to Ur et al.'s [58] recommendation of using less granular logs to make home-entryway surveillance less privacy invasive for teens. For example, an app may provide parents a high-level summary of who their teen is engaging with via their mobile device and how often, as opposed to divulging the content of every conversation (which current apps actually do [63]). For instance, the daughter who complained that her mother was stalking all her conversations with her friends, boyfriend, and biological dad, would then be able to reach some middle ground with her mother. Yes, the mother would know that her teen was conversing with her biological father and how often, but instead of reading the intimate details of the messages, the mother would have to ask her daughter if she had concerned. This type of privacy-preserving design would give parents a piece of mind while affording teens personal and psychological space.

Treating Teens as Agents of their Own Online Safety

An over-arching theme among many of the teen reviews is that teens did not like being treated like children. Therefore, we make the following recommendations targeted towards app designers to increase teen adoption and acceptance of mobile safety apps by thinking of teens as their end users: 1) Encourage teens to use mobile apps to self-regulate their own behaviors (as opposed to being forced to use an app by their parents), 2) provide features teens find personally beneficial, and 3) provide features so that teens can negotiate with parents. By taking a more "teen-centric" instead of a "parent-centric" approach to adolescent online safety, designers can help teens foster a stronger sense of personal agency for self-regulating their own online behaviors and managing online risks.

First, few teens are going to opt to install an app that explicitly says that it is for "parental control," which was the most common moniker shared among the apps reviewed. Therefore, the most simplistic design recommendation for prompting teens to use mobile online safety apps themselves would be to rebrand existing "parental control" apps to appeal directly to teens by setting the right tone for the target audience. Engaging with teens directly as end users may provide the cues that show teens they have agency and choice, thereby increasing their sense of personal autonomy and control.

Second, we should leverage user-centered techniques to better understand what mobile safety features teens would actually find useful [43]. Instead of assuming that teens are inherently risk-seeking, a more nuanced approach would be to *ask them* in what ways they feel that they need to be kept safe. For instance, we found that some teens liked apps that helped them disconnect from their phones or reduce other problematic behaviors. Therefore, teens may prefer "personal assistant" (e.g., [45]) type features that assist (not restrict) them in be more aware of their unhealthy behaviors and to change them without parental intervention. These features could keep track of teens' activities via their smart devices and "nudge" them whenever an inappropriate behavior is detected. Nudges appear to be at least somewhat effective in helping people to make better decisions [60], and should be examined in terms of efficacy with teen populations. In such cases, personal assistant features that serve to coach teens may serve as a replacement for parental surveillance, and thus, help solve the asymmetry problem between parents and teens.

Finally, in cases when teens' perceptions of appropriate mobile behaviors may conflict with their parents', it would be helpful for these apps to provide flexible parental controls that support and are more contingent on appropriate contexts of use [28], giving teens the ability to negotiate with their parents given particular circumstances. More app designs may consider implementing features similar to the “reward time system” offered by the Screen Time Companion App [71] that allowed teens to get extra time if they met certain criteria specified by their parents. Reward systems would be considered more contextualized restraints by providing positive reinforcement and allowing teens to earn privileges, as well as their parents’ trust [13,38]. Researchers who have studied more collaborative approaches between parents and teens [12,36] have found them to be more effective and achieve higher levels of “buy-in” from teens.

Limitations and Future Research

A key strength, but also a limiting factor of our study, is that we analyzed publicly posted reviews from Google Play that appeared to be made by children (ages 8-19). Since the meta-data surrounding the reviews was sparse, we only have limited insights as to the demographics of the participants in our sample. Only 17% of the reviews gave the child’s age with 56% of these reviews confirming that the reviewers were teens (ages 13-19) and 44% stating the child was a pre-teen (12 or younger). It was a design decision we made to leave the reviews made by younger children in our analysis as these reviews provided useful insights, including bringing light to the fact that mobile online safety is now a topic of interest for younger children, not just teens. Additionally, all reviews were written in English; therefore, we can assume that the large majority of these reviews were written by children in the United States or Europe. Hence, some of our parenting and privacy related findings may be more westernized in nature and may not be generalizable to other cultural contexts.

The dataset of child reviews was small compare to total user reviews (2.5% of all reviews). The significantly smaller percentage of child reviews could potentially be explained by the power differential between parents and teens [55]. Fear of parental reprimand may have dissuaded some teens from writing reviews. For this reason, we believe that our empirical evaluation of over 700 teen reviews, though it has limitations, serves as a baseline for future work for understanding mobile online safety apps from the perspective of children, at least those who were passionate enough to leave a review. Our findings provide valuable insights that can inform the next generation of mobile online safety apps. We encourage future research to build upon our findings by taking more direct approaches for soliciting feedback from children; for instance, using participatory design [2] to work with children as partners to conceptualize alternative solutions for designing mobile online safety apps.

CONCLUSION

Mobile technologies should support children in their developmental goals, including information-seeking, learning about rules and boundaries, and maintaining social relationships [7], in addition to keeping them safe from online risks. However, this goal will only be accomplished once designers listen more intently to children as end users. In the results presented in this paper, we chose to use a purely descriptive approach to present the key themes and unfiltered quotes from the child users. Our goal in doing this was to provide a non-judgmental account of what children had to say in their reviews. To conclude, however, we use a more interpretive lens to reflect on our results.

We observed a lot of frustration and anger in the child comments. Thus, it is possible that the reviews may have been overly biased toward negative impressions of the apps in an angered attempt to retaliate against their parents. However, the direct quotes from the child reviews actually illustrated a rather surprising level of maturity, self-awareness, and reason that researchers do not typically capture when viewing children through the eyes of adults. Children in our study wanted their parents to give them more freedom, a chance to prove they can make good online choices, and space to make some mistakes. They were not upset that online safety apps prevent them from risk-seeking behaviors; they were mad that they prevented them from doing other useful tasks.

Children liked features within apps that helped them with problematic behavior but gave them some level of control, or at least gave them a way to negotiate or compromise with their parents regarding rules and restrictions. Given this sociotechnical gap, children provided well-articulated and honest commentary around how these apps did not reinforce positive parenting practices and, based on the literature [62], they were right. These beneficial features are clearly under-supported within the existing app offerings [63]. Thus, our conclusion here was that we (as researchers, designers, and parents) might want to consider turning the critical lens around to look at ourselves and understand the negative biases we may hold about children when trying to keep them safe online.

REFERENCES

1. Monica Anderson. 2016. Parents, Teens and Digital Monitoring. *Pew Research Center: Internet, Science & Tech*. Retrieved July 12, 2016 from http://www.pewinternet.org/2016/01/07/parents-teens-and-digital-monitoring/
2. Zahra Ashktorab and Jessica Vitak. 2016. Designing Cyberbullying Mitigation and Prevention Solutions Through Participatory Design With Teenagers. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (CHI ’16), 3895–3905. https://doi.org/10.1145/2858036.2858548
3. Saeideh Bakhshi, Partha Kanuparthy, and David A. Shamma. 2015. Understanding Online Reviews: Funny, Cool or Useful? In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (CSCW ’15), 1270–1276. https://doi.org/10.1145/2675133.2675275
4. Eric P.S. Baumer, Phil Adams, Vera D. Khovanskaya, Tony C. Liao, Madeline E. Smith, Victoria Schwanda

Sosik, and Kaiton Williams. 2013. Limiting, Leaving, and (Re)Lapsing: An Exploration of Facebook Non-use Practices and Experiences. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '13), 3257–3266. https://doi.org/10.1145/2470654.2466446

5. Diana Baumrind. 1987. A developmental perspective on adolescent risk taking in contemporary America. *New Directions for Child and Adolescent Development* 1987, 37: 93–125. https://doi.org/10.1002/cd.23219873706
6. Diana Baumrind. 2005. Patterns of parental authority and adolescent autonomy. *New Directions for Child and Adolescent Development* 2005, 108: 61–69. https://doi.org/10.1002/cd.128
7. Lindsay Blackwell, Emma Gardiner, and Sarita Schoenebeck. 2016. Managing Expectations: Technology Tensions Among Parents and Teens. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (CSCW '16), 1390–1401.
8. Julie Boesen, Jennifer A. Rode, and Clara Mancini. 2010. The Domestic Panopticon: Location Tracking in Families. In *Proceedings of the 12th ACM International Conference on Ubiquitous Computing*, 65–74.
9. danah boyd. 2014. *It's Complicated: The Social Lives of Networked Teens*. Yale University Press, New Haven.
10. Toke Haunstrup Christensen. 2009. "Connected presence" in distributed family life. *New Media & Society* 11, 3: 433–451.
11. Lorrie Faith Cranor, Adam L. Durity, Abigail Marsh, and Blase Ur. 2014. Parents' and Teens' Perspectives on Privacy In a Technology-Filled World. In *Proceedings of the Tenth Symposium On Usable Privacy and Security*.
12. Alexei Czeskis, Ivayla Dermendjieva, Hussein Yapit, Alan Borning, Batya Friedman, Brian Gill, and Tadayoshi Kohno. 2010. Parenting from the Pocket: Value Tensions and Technical Directions for Secure and Private Parent-teen Mobile Safety. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (SOUPS '10), 15:1–15:15. https://doi.org/10.1145/1837110.1837130
13. Marie Drolet and Isabelle Arcand. 2013. Positive Development, Sense of Belonging, and Support of Peers among Early Adolescents: Perspectives of Different Actors. *International Education Studies* 6, 4: 29. https://doi.org/10.5539/ies.v6n4p29
14. Wenjing Duan, Bin Gu, and Andrew B. Whinston. 2008. Do online reviews matter? — An empirical investigation of panel data. *Decision Support Systems* 45, 4: 1007–1016. https://doi.org/10.1016/j.dss.2008.04.001
15. Daniel A. Epstein, Bradley H. Jacobson, Elizabeth Bales, David W. McDonald, and Sean A. Munson. 2015. From "Nobody Cares" to "Way to Go!": A Design Framework for Social Sharing in Personal Informatics. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (CSCW '15), 1622–1636. https://doi.org/10.1145/2675133.2675135
16. Lee B. Erickson, Pamela Wisniewski, Heng Xu, John M. Carroll, Mary Beth Rosson, and Daniel F. Perkins. 2016. The boundaries between: Parental involvement in a teen's online world. *Journal of the Association for Information Science and Technology* 67, 6: 1384–1403.
17. Jennifer Fereday and Eimear Muir-Cochrane. 2008. Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development. *International Journal of Qualitative Methods - ARCHIVE* 5, 1: 80–92.
18. Colin Fitzpatrick, Jeremy Birnholtz, and Darren Gergle. 2016. People, Places, and Perceptions: Effects of Location Check-in Awareness on Impressions of Strangers. In *Proceedings of the 18th International Conference on Human-Computer Interaction with Mobile Devices and Services* (MobileHCI '16), 295–305. https://doi.org/10.1145/2935334.2935369
19. Bin Fu, Jialiu Lin, Lei Li, Christos Faloutsos, Jason Hong, and Norman Sadeh. 2013. Why People Hate Your App: Making Sense of User Feedback in a Mobile App Store. In *Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (KDD '13), 1276–1284.
20. Kentaro Fujita and Joseph C. Roberts. 2010. Promoting prospective self-control through abstraction. *Journal of Experimental Social Psychology* 46, 6: 1049–1054.
21. Daniel Gerdes and James H. Conn. 2001. A User-Friendly Look at Qualitative Research Methods. *Physical Educator* 58, 4: 183.
22. Giovanna Mascheroni and Kjartan Ólafsson. 2016. The mobile Internet: Access, use, opportunities and divides among European children. *New Media & Society* 18, 8: 1657–1679. https://doi.org/10.1177/1461444814567986
23. Shion Guha and Jeremy Birnholtz. 2013. Can You See Me Now?: Location, Visibility and the Management of Impressions on Foursquare. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services* (MobileHCI '13), 183–192. https://doi.org/10.1145/2493190.2493209
24. Shion Guha and Stephen B. Wicker. 2015. Spatial Subterfuge: An Experience Sampling Study to Predict Deceptive Location Disclosures. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (UbiComp '15), 1131–1135. https://doi.org/10.1145/2750858.2804281

25. Shion Guha and Stephen B. Wicker. 2015. Do Birds of a Feather Watch Each Other?: Homophily and Social Surveillance in Location Based Social Networks. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (CSCW '15), 1010–1020. https://doi.org/10.1145/2675133.2675179

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

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

28. Alexis Hiniker, Sarita Y. Schoenebeck, and Julie A. Kientz. 2016. Not at the Dinner Table: Parents' and Children's Perspectives on Family Technology Rules. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (CSCW '16), 1376–1389.

29. Leonard Hoon, Rajesh Vasa, Gloria Yoanita Martino, Jean-Guy Schneider, and Kon Mouzakis. 2013. Awesome!: Conveying Satisfaction on the App Store. In *Proceedings of the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration* (OzCHI '13), 229–232. https://doi.org/10.1145/2541016.2541067

30. Nan Hu, Indranil Bose, Noi Sian Koh, and Ling Liu. 2012. Manipulation of online reviews: An analysis of ratings, readability, and sentiments. *Decision Support Systems* 52, 3: 674–684. https://doi.org/10.1016/j.dss.2011.11.002

31. Nan Hu, Paul A. Pavlou, and Jennifer Zhang. 2006. Can Online Reviews Reveal a Product's True Quality?: Empirical Findings and Analytical Modeling of Online Word-of-mouth Communication. In *Proceedings of the 7th ACM Conference on Electronic Commerce* (EC '06), 324–330. https://doi.org/10.1145/1134707.1134743

32. Nan Hu, Jie Zhang, and Paul A. Pavlou. 2009. Overcoming the J-shaped Distribution of Product Reviews. *Commun. ACM* 52, 10: 144–147. https://doi.org/10.1145/1562764.1562800

33. Gregor Jawecki and Johann Fuller. 2008. How to use the innovative potential of online communities? Netnography – an unobtrusive research method to absorb the knowledge and creativity of online communities. *International Journal of Business Process Integration and Management* 3, 4: 248–255. https://doi.org/10.1504/IJBPIM.2008.024982

34. Haiyan Jia, Pamela J. Wisniewski, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2015. Risk-taking As a Learning Process for Shaping Teen's Online Information Privacy Behaviors. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (CSCW '15), 583–599.

35. Carrie D. Kennedy-Lightsey and Brandi N. Frisby. 2016. Parental Privacy Invasion, Family Communication Patterns, and Perceived Ownership of Private Information. *Communication Reports* 29, 2: 75–86. https://doi.org/10.1080/08934215.2015.1048477

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

37. Nikolaos Korfiatis, Elena García-Bariocanal, and Salvador Sánchez-Alonso. 2012. Evaluating content quality and helpfulness of online product reviews: The interplay of review helpfulness vs. review content. *Electronic Commerce Research and Applications* 11, 3: 205–217. https://doi.org/10.1016/j.elerap.2011.10.003

38. Ben M. F. Law, Andrew M. H. Siu, and Daniel T. L. Shek. 2012. Recognition for Positive Behavior as a Critical Youth Development Construct: Conceptual Bases and Implications on Youth Service Development. *The Scientific World Journal* 2012: e809578. https://doi.org/10.1100/2012/809578

39. Sonia Livingstone and Peter K. Smith. 2014. Annual Research Review: Harms experienced by child users of online and mobile technologies: the nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of Child Psychology and Psychiatry* 55, 6: 635–654. https://doi.org/10.1111/jcpp.12197

40. Sonya Livingstone. 2008. Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy, and self-expression. *New Media & Society* 10: 393–411.

41. Alice Marwick. 2012. The Public Domain: Surveillance in Everyday Life. *Surveillance & Society* 9, 4: 378–393.

42. Alice E Marwick and danah boyd. 2014. Networked privacy: How teenagers negotiate context in social media. *New Media & Society* 16, 7: 1051–1067. https://doi.org/10.1177/1461444814543995

43. Karsten Nebe and Dirk Zimmermann. 2007. Aspects of Integrating User Centered Design into Software Engineering Processes. In *Human-Computer Interaction. Interaction Design and Usability*, 194–203. https://doi.org/10.1007/978-3-540-73105-4_22

44. Helen Nissenbaum. 2004. PRIVACY AS CONTEXTUAL INTEGRITY. *Washington Law Review* 79, 119.

45. Ardis L. Olson, Cecelia A. Gaffney, Pamela W. Lee, and Pamela Starr. 2008. Changing Adolescent Health Behaviors. *American Journal of Preventive Medicine* 35, 5: S359–S364. https://doi.org/10.1016/j.amepre.2008.08.014

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

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

48. 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.

49. Sandra Sporbert Petronio. 2002. *Boundaries of Privacy: Dialects of Disclosure*. SUNY Press.

50. Anthony T. Pinter, Pamela Wisniewski, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2017. Adolescent Online Safety: Moving Beyond Formative Evaluations to Designing Solutions for the Future. In *Proceedings of the International Conference on Interaction Design and Children*.

51. Erika S. Poole and Tamara Peyton. 2013. Interaction Design Research with Adolescents: Methodological Challenges and Best Practices. In *Proceedings of the 12th International Conference on Interaction Design and Children* (IDC '13), 211–217.

52. Rivka Ribak. 2009. Remote control, umbilical cord and beyond: the mobile phone as a transitional object. *The British Journal of Developmental Psychology* 27, Pt 1: 183–196.

53. Jennifer A. Rode. 2009. Digital Parenting: Designing Children's Safety. In *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology* (BCS-HCI '09), 244–251.

54. Stefan Siersdorfer, Sergiu Chelaru, Wolfgang Nejdl, and Jose San Pedro. 2010. How Useful Are Your Comments?: Analyzing and Predicting Youtube Comments and Comment Ratings. In *Proceedings of the 19th International Conference on World Wide Web* (WWW '10), 891–900.

55. Yvette Solomon, Jo Warin, Charlie Lewis, and Wendy Langford. 2002. Intimate Talk between Parents and their Teenage Children: Democratic Openness or Covert Control? *Sociology* 36, 4: 965–983. https://doi.org/10.1177/003803850203600409

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

57. Anselm Strauss and Juliet Corbin. 1998. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. SAGE Publications, Inc, Thousand Oaks.

58. Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders Versus Intrusiveness: Teens' and Parents' Perspectives on Home-entryway Surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (UbiComp '14), 129–139. https://doi.org/10.1145/2632048.2632107

59. Rajesh Vasa, Leonard Hoon, Kon Mouzakis, and Akihiro Noguchi. 2012. A Preliminary Analysis of Mobile App User Reviews. In *Proceedings of the 24th Australian Computer-Human Interaction Conference* (OzCHI '12), 241–244. https://doi.org/10.1145/2414536.2414577

60. Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. 2014. A Field Trial of Privacy Nudges for Facebook. In *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems* (CHI '14), 2367–2376. https://doi.org/10.1145/2556288.2557413

61. Robert S. Weisskirch. 2009. Parenting by cell phone: parental monitoring of adolescents and family relations. *Journal of Youth and Adolescence* 38, 8: 1123–1139.

62. Sarah Whittle, Julian G. Simmons, Meg Dennison, Nandita Vijayakumar, Orli Schwartz, Marie B. H. Yap, Lisa Sheeber, and Nicholas B. Allen. 2014. Positive parenting predicts the development of adolescent brain structure: A longitudinal study. *Developmental Cognitive Neuroscience* 8: 7–17. https://doi.org/10.1016/j.dcn.2013.10.006

63. Pamela Wisniewski, Arup Kumar Ghosh, Mary Beth Rosson, Heng Xu, and John M. Carroll. 2017. Parental Control vs. Teen Self-Regulation: Is there a middle ground for mobile online safety? In *Proceedings of the 20th ACM Conference on Computer Supported Cooperative Work & Social Computing*.

64. Pamela Wisniewski, Haiyan Jia, Na Wang, Saijing Zheng, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2015. Resilience Mitigates the Negative Effects of Adolescent Internet Addiction and Online Risk Exposure. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (CHI '15), 4029–4038. https://doi.org/10.1145/2702123.2702240

65. Pamela Wisniewski, Mary Beth Rosson, Heng Xu, and John M. Carroll. 2017. Parents Just Don't Understand: Why Teens Don't Talk to Parents about Their Online Risk Experiences. In *Proceedings of the 20th ACM Conference on Computer Supported Cooperative Work & Social Computing*.

66. Pamela Wisniewski, Heng Xu, Jack Carroll, and Mary Beth Rosson. 2013. Grand Challenges of Researching Adolescent Online Safety: A Family Systems Approach. *AMCIS 2013 Proceedings*. Retrieved from http://aisel.aisnet.org/amcis2013/SocialTechnicalIssues/GeneralPresentations/10

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

68. Y. Zhang and B.M. Wildemuth. 2009. Qualitative analysis of content. *Applications of social research methods to questions in information and library science*: 308–319.

69. 2013. Children's Online Privacy Protection Rule ("COPPA"). *Federal Trade Commission*. Retrieved August 1, 2017 from https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

70. Downloading App Store & Google Play reviews made easy. Retrieved August 8, 2016 from http://heedzy.com/feedback#

71. Screen Time Parental Control - Android Apps on Google Play. Retrieved August 6, 2016 from https://play.google.com/store/apps/details?id=com.screentime.rc