Co-designing Mobile Online Safety Applications with Children

Brenna McNally[1], Priya Kumar[1], Chelsea Hordatt[1], Matthew Louis Mauriello[2], Shalmali Naik[1], Leyla Norooz[1], Alazandra Shorter[1], Evan Golub[2], Allison Druin[1]
Human-Computer Interaction Lab (HCIL)
College of Information Studies[1], Department of Computer Science[2]
University of Maryland, College Park
{bmcnally, pkumar12, adruin}@umd.edu

ABSTRACT
Parents use mobile monitoring software to observe and restrict their children's activities in order to minimize the risks associated with Internet-enabled mobile devices. As children are stakeholders in such technologies, recent research has called for their inclusion in its design process. To investigate children's perceptions of parental mobile monitoring technologies and explore their interaction preferences, we held two co-design sessions with 12 children ages 7-12. Children first reviewed and redesigned an existing mobile monitoring application. Next, they designed ways children could use monitoring software when they encounter mobile risks (*e.g.,* cyberbullying, inappropriate content). Results showed that children acknowledged safety needs and accepted certain parental controls. They preferred and designed controls that emphasized restriction over monitoring, taught risk coping, promoted parent-child communication, and automated interactions. Our results benefit designers looking to develop parental mobile monitoring technologies in ways that children will both accept and can actively benefit from.

Author Keywords
Co-design; children; online safety; mobile applications

ACM Classification Keywords
H.5.m. Information interfaces and presentation (*e.g.,* HCI): Miscellaneous;
K.4.1 Public Policy Issues: Human safety, Privacy

INTRODUCTION
Mobile technologies have made their way into our homes, into our lives, and into children's pockets. In the U.S., 98% of children under age 9 have home access to a mobile device [9], and children who receive their own devices are, on average, 10 years old [40]. Internet access—particularly the anytime, anywhere access that mobile devices provide—presents many opportunities for children. Mobile devices provide children a convenient method to communicate with family and friends, earn parental trust, and learn responsibility [29]. They also offer opportunities for safety [12], learning [23], and entertainment [30].

Figure 1. Children reviewing and redesigning how features of a parental mobile monitoring application should work during a co-design session.

Along with these opportunities, children's increasing access to Internet-connected mobile devices means that Internet- and communication-related risks become more persistent in their lives. Risks related to children's Internet access include *content threats* (*e.g.,* inappropriate ads), *contact threats* (*e.g.,* cyberbullying, predators), *conduct threats* (*e.g.,* illegal file sharing), and *computer threats* (*e.g.,* phishing) [21]. While children as young as 5 years old develop an awareness of these risks and practice risk-mitigation strategies [24], mobile monitoring technologies offer safety-conscientious parents unprecedented abilities to reduce risk exposure. For instance, parents who are

CHI 2018, April 21–26, 2018, Montreal, QC, Canada

ACM ISBN 978-1-4503-5620-6/18/04…$15.00
https://doi.org/10.1145/3173574.3174097

concerned about their children accessing inappropriate content may restrict application downloads or Internet access on their children's mobile devices.

While potentially protecting children from the risks associated with access to mobile technologies, these solutions may also have adverse side effects. If Internet access is over-restricted it may compromise the child's ability to complete homework or pursue personal interests [16]. Moreover, children who feel like their privacy is being invaded may find ways to avoid being monitored [3,13], negating the goals of the software.

Despite the impacts that monitoring and restrictions have on children's use of mobile technologies, few studies look at children's desires regarding these monitoring technologies. Notable works tend to focus on teenagers (*i.e.,* those ages 13-19) within domains such as cyberbullying [2,7]. To develop tools that children (*i.e.,* those under age 13) and parents will both use and benefit from, researchers have recently called for acquiring children's input on the design of mobile monitoring software [21,34].

To understand children's perceptions and obtain their input on parental mobile monitoring applications, we conducted two co-design sessions with 12 children ages 7-12. We investigated: *To what extent do children consider different parental mobile monitoring activities appropriate? What mobile monitoring interventions do children desire and envision using?* All children were surveyed on whether features in an existing parental mobile monitoring application (*e.g.,* tracking location, reading text messages) are appropriate. They were then asked to redesign the features as they saw fit. Eight children additionally prototyped ways mobile monitoring applications could be used during *content* and *contact threat* situations. To further contextualize findings from these two co-design activities, we coded the application features children designed using the Teen Online Safety Strategies (TOSS) Framework [34]—which characterizes features that support mobile online safety in terms of *parental control* vs *self-regulation* (Table 1). While the TOSS framework was developed with teenagers in mind, it broadly characterizes strategies for mediating online safety that are likely to be relevant to children of all ages.

Findings from this work reveal that our child co-designers acknowledge mobile safety risks and accept certain parental controls. Our study also suggests children prefer restriction over monitoring features. Moreover, they envision futures where the software applies automation to help mitigate and detect risk, teaches risk coping techniques, and encourages parent-child communication to improve their experience of using mobile devices. Our results inform designers looking to develop parental mobile monitoring technologies in ways that children will both accept and can actively benefit from. Finally, our study demonstrates that the TOSS framework, originally designed for use with teenagers, can also inform online safety efforts involving children.

Teen Online Safety Strategies (TOSS) Conceptual Framework

Parental Control		Teen Self-Regulation
Monitoring: Passive surveillance of a teen's online activities		**Self-Monitoring:** Awareness of one's own motivations and actions through self-observation
Restriction: Placing rules and limits on a teen's online activities		**Impulse Control:** Inhibiting one's short-term desires in favor of long-term consequences
Active Mediation: Discussions between parents and teens regarding online activities	⟷	**Risk Coping:** Managing a negative event once it has occurred

Table 1. The Teen Online Safety Strategy [TOSS] framework, developed by Wisniewski et. al [34].

RELATED WORK

Here, we survey related work on (i) children's mobile use, (ii) current monitoring strategies, and (iii) the effects and effectiveness of mobile monitoring practices.

Children's Mobile Use

The convenience and opportunities that mobile devices offer children have encouraged parents to purchase personal devices for their children. Both parents and children appreciate the entertainment and communication value that these devices provide [6,13]. However, reactions to children's use of these devices have been mixed. Debates about how screen time affects children's physical and social development are common in literature and the media [1,5]. Parents worry about children's intentional and unintentional access to inappropriate content, strangers' ability to contact their children, depression, cell phone addiction, and bullying [2,8,33]. Recent research gives credence to some of these concerns; for instance, accessing image-sharing mobile applications (*e.g.*, Snapchat, Instagram) may increase the chances that a child will experience cyberbullying [14]. Our work is predicated upon children's use and ownership of mobile devices, and the complicated relationship between the technology's benefits and risks.

Monitoring and Mediation

Managing children's technology use is a dynamic, contextually driven process [26,28], and the processes families enact to manage household technologies are as varied as family life. Across a sample of 12 families, Rode uncovered five strategies parents use to manage children's technology use [28]. Some parents monitored children without using technology while others did so with the support of technical tools; some parents encouraged their children to practice self-regulation while others blocked their children from engaging in specific activities. Many parental risk-mitigation strategies focus on these types of *activity constraints* (*e.g.,* no Snapchat) or on *context constraints* (*e.g.,* limiting screen time) [22].

The TOSS framework characterizes approaches and practices around online safety as either *parental control* or *self-regulation* strategies (Table 1) [34]. The strategies that mobile monitoring applications employ generally emphasize *parental control*, with features that screen the

contacts or applications on a child's device, read a child's communications (*e.g.,* text messages, social media posts), check a child's browsing history, or require a child to share account passwords [1,10,38,39]. Features of mobile apps that support parents in monitoring and mediating their children's mobile device use tend to prioritize the *monitoring* and *restriction* aspects of *parental control* over other strategies that would promote *self-regulation* [34].

Despite the fact that elementary school-age children recognize how privacy and security threats can emerge when using digital devices [24,39], studies show that parents struggle to enforce technology rules with their children [4,22,26,28,38]. Additionally, children's desire for privacy and autonomy, as reflected in online safety strategies related to self-regulation, can play a part in challenges to parental mediation and monitoring strategies [35]. While both children and parents largely recognize a child's right to privacy and its limits [24], their opinions diverge about how to negotiate it in digital spaces. Teenagers, for instance, may not oppose parental monitoring but prefer systems where they are aware of the system, receive notifications when parents access information, and control some aspects of data sharing [11]. Children also develop strategies to resist parental mobile monitoring, such as ignoring phone calls but telling parents they didn't hear it ring, saying that their phone's battery died or that their phone was off, or writing text messages to friends in a covert language so that parents can't decipher the messages [3,13]. As there have been several recent calls to investigate how children perceive the acceptability of existing monitoring and mediation applications [21,34], our work begins to address this missing perspective in parental mobile monitoring literature.

Effectiveness and Effects of Monitoring

The links between parental mediation and the reduction of online risk are complicated. Livingstone & Helsper found that while parents preferred active co-use strategies (*e.g.,* staying nearby when children go online, discussing online activities) over monitoring children's Internet use (*e.g.,* using monitoring software or reading a child's emails), neither effectively reduced children's exposure to online risks [25]. Parental restriction of interactions or activities (*e.g.*, prohibiting instant messaging services or games) did reduce children's online risk exposure, but it is precisely these activities that attract children to the Internet [16,25]. Wisniewski *et al.* suggest that a combination of direct intervention (*e.g.,* use of parental controls) and active mediation (*e.g.,* discussing technology use with children) best balances mitigating online risks while enabling children to take advantage of technology [35].

Regardless of effectiveness, children and parents may experience unanticipated negative effects of monitoring and mediation practices. While tracking children's mobile use activities can foster compliance, it removes the opportunity for a child to demonstrate responsibility and earn trust [29]. Similarly, children who avoid a particular behavior because they know their parents will find out demonstrate that they can avoid detection and punishment, not that they can use technology responsibly [21,29]. Parents, too, are affected by the incorporation of monitoring and mediation technologies into family life. The notion that parents should monitor their children's technology use pervades, particularly in Western societies where risk-aversion or surveillance can become a norm [18,27]. Yet parents may find these technologies to be "burdensome and ineffective" [21,38 p.3241] or too rigid for the contextual nature of children's everyday technology use [26]. Moreover, parents might not be capable of effectively evaluating threats or understanding privacy implications [19,36]. In our work, we begin to explore children's desires for how mobile monitoring technology could reflect their desires and assist them effectively in risk situations.

STUDY METHOD

To investigate children's perceptions of and desires for mobile monitoring technologies, we held two Cooperative Inquiry (CI) co-design sessions [15,20] with the University of Maryland's Kidsteam.

Process. In CI, a team of adult researchers and about eight children, ages 7-11, work together as design partners to create technologies that are more relevant to children's wants and needs [17,20]. Children on the Kidsteam CI design team participate in twice-weekly design sessions throughout an academic year. Both co-design sessions were held at the University of Maryland's Human-Computer Interaction Lab (HCIL), lasted 90 minutes, and followed a similar schedule: After being introduced to the design prompt and activity, small groups of 2-3 children and 1-2 adults were formed to complete the design tasks. After the design activity, the groups presented their ideas to the rest of the team. An adult researcher wrote down the ideas from each group on a whiteboard and rapidly derived themes across the groups' ideas, which the team then discussed at the end of the session. Adult design partners discussed and iterated upon these themes after the session ended.

In this work we first describe the two co-design activities and their findings. Additionally, we analyze the features children designed during both activities using the TOSS framework to better understand the intervention strategies children desire.

Participants. Our two co-design sessions were held across two academic years; 4 children did not return to the team between years, and new children joined the team. Consequently, all 12 children (ages 7-12, 8 female) completed the survey and redesign activity that was conducted at both design sessions, and 8 children completed the additional content and contact threat activity that was held during the second co-design session (Table 2). Given their membership on a technology design team, participants had a moderately high comfort level with technology use. Participants also had varied educational

Participant ID#	Gender	Activity #1: Survey & Redesigns		Activity #2: Designs for Threats	
		Completed	Years Old	Completed	Years Old
P1*	F	✓	7	✓	7
P2	F	✓	9	✓	10
P3	F	✓	9	✓	10
P4*	F	✓	9	✓	9
P5	F	✓	9	✓	10
P6	F	✓	10		
P7	F	✓	11		
P8	F	✓	12		
P9	M	✓	7	✓	8
P10	M	✓	8		
P11*	M	✓	10	✓	10
P12*	M	✓	11	✓	11

*Participants in the second co-design session, only; completed both activities.

Table 2. Demographics of the children who participated in each of the activities during the two 2 co-design sessions.

backgrounds—being homeschooled (1), attending public schools (8), and private schools (3).

CO-DESIGN ACTIVITY #1: SURVEY AND FEATURE REDESIGN

This activity, conducted at both co-design sessions (Table 2), first asked children to review the features of TeenSafe [41], a commercially available parental mobile monitoring application that was unfamiliar to the children. "*Built by parents, for parents"* [34], the app exemplifies the features that parents desire and employ (*e.g.,* allowing parents to monitor and restrict what children do on their iPhones). While the app is marketed for teenagers, its online parenting guide offers advice on technology use and monitoring for children as young as 6 years old.

To review the application, the children completed a survey about 10 of its features (three restriction-based, seven monitoring-based). For each feature, they were also asked whether "parents *should* or *should not* be able to control this feature" (*e.g.,* view children's contacts, read children's text messages, restrict app downloads). Our co-designers then had the option to redesign features they thought parents "should not" be able to control by drawing new mockups (Figure 1).

Analysis

We analyzed children's survey data and report the percent and number of participants who expressed agreement for each of the 10 application features (Figure 2). Given the small sample size, we refrain from reporting any other statistical analyses. We complement our results with quotes illustrating the children's reasoning and the children's design suggestions for the features they redesigned. Child participants are identified by a "P" followed by a numerical identifier (*e.g.,* P3; Table 2).

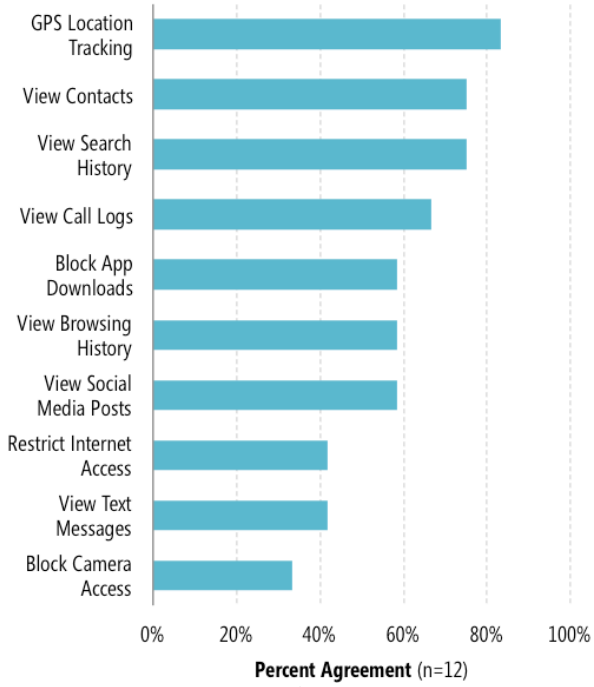

Figure 2. Results of the survey children took on whether parents should have access to features provided by mobile monitoring applications.

Findings

Monitoring Features

Seven of the surveyed features focused on monitoring how children use their mobile device. The monitoring feature that children felt was most acceptable was letting parents *see your location,* with 83% (10/12) of the children agreeing that parents should have this access. As P12 described, parents need "*to see if [kids] are robbed or kidnapped."* The two children disagreed did so because they were already required to tell their parents their whereabouts and did not see the value of additional monitoring. Similarly, most children (75%, 9/12) thought parents should be able to *see their contacts* in case of danger—*"What if there is a stranger on your contacts?"* (P2)—as well as *see their call logs* (67%, 8/12). Nevertheless, one participant noted the redundancy of parents having the ability to monitor children's contacts as well as their call logs, and determined that parents should not be able to see call logs because, *"They know everyone [children would be calling] anyway"* (P4).

Monitoring *search history* was considered acceptable by 75% (9/12) of the children and monitoring the *browsing history* was considered acceptable by 58% (7/12) of the children. However, one participant described a fear of mistakenly getting into trouble as the reason why parents should not be able to monitor these activities: "*What you are doing could be taken the wrong way. Like going to a drug use website for a health class project"* (P7). More than half of the children (58%, 7/12) thought parents should be able to *view all their social media activities* (*e.g.,* posts,

messages, comments), because parents *"should know what [their children] are looking at"* (P8) and posts *"could be seen by anyone"* (P7).

Regarding whether parents should be able to read children's text messages, 42% (5/12) of children thought parents should have this ability. P10 qualified his agreement, stating that parents should only be notified if there is a "bad" text and should not get full access to the messages.

Restriction Features

Three of the surveyed features focused on restriction. These included limiting or restricting camera access, Internet access, and the ability to use or download applications.

When asked whether parents should be able to *restrict what apps are downloaded* to their device, 58% (7/12) of children agreed. Those who did not believe parents should be able to restrict the feature redesigned the capability, adding granularity such as "no in-app purchases" or restricting access to specific application downloads.

Less than half of the children (42%, 5/12) believed parents should be able to *restrict their access to the Internet* on their mobile devices. Children who opposed blanket restrictions on Internet access designed features such as optional restrictions on websites (e.g., blocking URLs, age-based maturity settings).

The least acceptable restriction was *camera use,* with 33% (4/12) of the children agreeing that parents should be able to turn off the camera on children's devices. However, P10 felt parents should be able to turn off the camera because, *"people are weird."* The children who did not believe parents should be able to restrict camera use designed different levels of restriction in their mockups, but did not entirely remove the capability. For instance, they offered parents the ability to restrict interactive camera uses (*e.g.,* video chatting) while leaving picture-taking enabled.

Active Mediation

While none of the surveyed features promoted active mediation, several feature re-designs incorporated this type of parental control. When surveyed about restricting Internet access, P4 suggested that parents, *"just talk to the child."* Similarly, P7 desired active mediation with regard to restricting Internet access and blocking mobile application downloads. P7 designed "Ask Child" and "Consult Kid" buttons for parents to use before taking these actions, explaining: *"Instead of it being forced and kids having no say, consult [them]"* (P7).

CO-DESIGN ACTIVITY #2: DESIGNS FOR MOBILE THREATS

During the second activity, conducted during the second co-design session, the children (n=8, Table 2) participated in a Big Paper paper-prototyping activity [32] where they designed mobile interfaces that would help children handle commonly discussed mobile issues. Children were first presented with a *content threat* scenario—accidental exposure to inappropriate material online—and then with a *contact threat* scenario—cyberbullying via instant messaging—and asked to "design a mobile monitoring application that could help children who encounter these situations." The research team chose these scenarios as they represent common mobile Internet threats.

Analysis

As part of the CI method, the big ideas that small groups presented at the end of the activity were thematically analyzed by an adult researcher at the end of the session, which identified patterns as well as unique design ideas [17]. The entire team discussed these themes before the children left the design session, and the adult design partners later iterated on the themes.

Findings

The themes that emerged from this design session included *automatic technology interventions* and *immediate incident management assistance*.

Automatic Technology Interventions

Children's designs incorporated automatic interventions across features focused on both self-regulation and parental control. For instance, children designed features for the automatic restriction of contacts when a threat was encountered, a task usually designated to parents:

> *"So, if somebody says a bad word [the app] will automatically say, 'This person said a bad word. He or she will be blocked so that person can't talk with you anymore'"* (P9).

Similarly, children removed the need for direct parental monitoring of their activities through designs for automated message filtering:

> *"If we had a bad text then there would be an X and when the person sends it to you it wouldn't show up to you, but the X would show up on their screen and it would give them an alert so that they couldn't do it"* (P11).

Children also designed features that would offer partially automated parental monitoring, such as a parental notification system that applied automatic detection to apprise parents of text message content only when potential risks were identified:

> *"If it's a bad text, the text would go to the parent's [device] first to see if their kid can read it. […] Then [parents] can say, 'don't approve' or 'approve' text. Basically like a filter"* (P12).

Immediate Incident Management Assistance

While children designed many features focused on automation, the designs they developed to address the *content* and *contact threat* scenarios more specifically emphasized either *restriction* (to prevent exposure) or offered children *risk-coping* strategies. The risk-coping strategies often offered immediate interventions to help children feel better, such as cat videos to watch or suggestions that the child go play with a sibling.

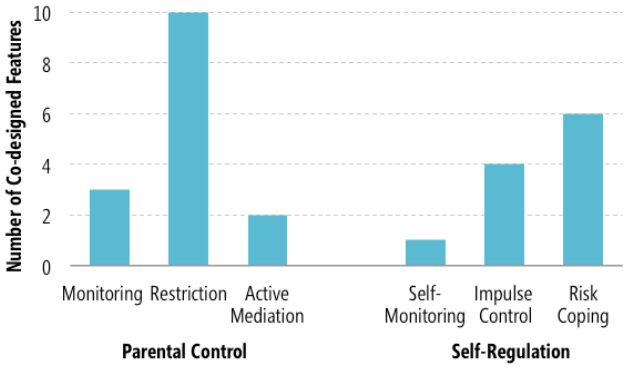

Figure 3. Categorization of the features children co-designed into the TOSS Framework.

Additionally, all designs featured special sets of emojis that children could send to *"show your disapproval"* (P1). These emojis would immediately appear if the child received a harsh message and offered children appropriate, effective ways to respond to the contact threat. In the case of the cyberbullying prompt, other risk-coping suggestions emphasized children's future experiences and behaviors, such as offering children ways to respond if they saw the person who was cyberbullying them in person: *"Once you block someone, it gives you suggestions on what to do if you see them afterward"* (P5).

CROSS-ACTIVITY FEATURE ANALYSIS

The parental mobile monitoring applications that are currently available, including the one that children reviewed in Activity 1, almost exclusively offer monitoring and restriction features [34]. To further categorize and describe what types of features children desire, we coded the features they designed during both of the co-design sessions using the TOSS framework.

Analysis

Our analysis began by compiling transcribed presentation videos, observational notes, photographs of the design artifacts, and the debrief write-ups from the two sessions. We sampled 20% of the compiled data and two researchers deductively coded the features children designed using the TOSS framework [34] (Table 1). We then calculated Inter-Rater Reliability and achieved an average Cohen's kappa of .89, as calculated by NVivo software, considered *almost perfect agreement* (range: .81-.99) [31]. After resolving differences in coding, the remaining data were divided between the two researchers and coded separately.

Findings

Figure 3 illustrates the proportion of the features children generated across the *parental control* and *self-regulation* dimensions of the TOSS framework. Within the dimension of parental control, children's designs illustrated a strong preference toward restriction of activities over monitoring of activities. While features in commercial mobile monitoring applications rely heavily on parental control [34], children's designs incorporated a more balanced feature set between the parental control and self-regulation dimensions. Designs for self-regulation emphasized the inclusion of risk-coping features as well as impulse control features. Features promoting active mediation and self-monitoring were the least commonly designed.

DISCUSSION

In this work we conducted two co-design activities to better understand children's perceptions of parental mobile monitoring technology. While children's voices have rarely been considered when it comes to the design of these applications—and thus the features available in the applications reflect the goals and desires of adult, generally parent, perspectives—this work answers a call to give children a voice in designing these technologies [21,34]. By including children as stakeholders, our work envisions new futures and properties for mobile monitoring technologies, suggesting that the scope of these technologies can be expanded and designed in ways that children will both accept and from which they can actively benefit. Here, we discuss children's (i) mobile monitoring preferences, (ii) the solutions they propose to address their preferences, and finally (iii) reflect on the utility of applying the TOSS framework to this context. We also discuss limitations to generalizability and the need for future investigations.

Children's Mobile Monitoring Preferences

The children in our design sessions understood parents' desires for certain types of oversight. Previous research has shown that children acknowledge the need for online safety [21,24] and understand that being online includes risks [24]. The children in our co-design sessions displayed similar attitudes and they acknowledged the need for parental assistance through designs that gave up some of children's personal privacy to enable parental mobile monitoring activities. This was particularly evident with features relating to children's physical protection (*e.g.,* GPS tracking children's physical locations). However, there were limits to what children found acceptable in terms of impositions on their privacy, even in the name of their own protection. These limits were demonstrated by their design of features that provided non-parental support through automated and self-regulation strategies.

Children's Mobile Monitoring Solutions

Children envisioned mobile monitoring applications as more than passive tools. By leveraging the access to children's data that these tools already have, children envisioned technology that could do more than monitor and restrict their activities: it could also teach them skills and help them cope with risk situations. They designed technologies that provide (i) interactive features, (ii) opportunities to learn about risks and privacy concerns, and (iii) methods to cope with risks they encounter. Similar to the "designs for support" that teenagers have co-designed to address cyberbullying incidents [2], many of these children's designs had features that would notify and correct children (and their peers) who engage in harmful behaviors (*e.g.,* sending inappropriate messages) or teach

them to develop coping mechanisms (*e.g.,* taking a break from the device, switching activities, learning to block harassers). Other designs included children in conversations about their technology use with parents before restrictions were put into place. Echoing tensions regarding children's online safety [21], children's emphasis on self-regulatory features moves away from the common, often exclusive, focus on parental control seen in existing mobile monitoring applications and starts to ask for parental trust.

Children's emphasis on greater balance between parent control and self-regulation features within parental mobile monitoring software applications highlights the gap between existing parental mobile monitoring applications [34] and what children desire. While children acknowledge the value of parental control, they also seek a measure of privacy in their mobile activities. This is to be expected, and likely to be more pronounced as children age. Younger children tend to view privacy in terms of being alone, managing information, and controlling access to places. However, as children grow older they start to understand the role of privacy in autonomy [37]. Some straightforward ways that children's designs addressed the gap between existing mobile monitoring features and their own preferences include emphasizing the use of restriction over monitoring features. Others designs they created would require a greater change in perspective on how parental mobile monitoring should be approached, such as children's desire for automated, in-the-moment assistance when they encounter risk situations. This greater range of feature offerings could create congruence between mobile monitoring activities and the highly varied ways families manage technology use [38]. Moreover, the incorporation of automated or semi-automated monitoring approaches could simultaneously help protect children while maintaining a layer of privacy, offer time savings for parents, and scaffold building trust and learning self-regulatory processes [24].

Reflection on Method

The TOSS framework was developed to describe mobile online safety strategies of adolescents [34]. It has previously been used to conduct a feature analysis of existing teen online safety mobile applications, helping to surface themes that described the values within the applications [34]. In this work we expanded on the application of the TOSS framework, demonstrating that (i) it was robust enough to apply to a feature analysis of technologies meant for younger children and (ii) that valuable insights could be acquired using the framework for a feature analysis of co-designed artifacts.

Limitations and Future Work

This study was conducted during two, 90-minute design sessions with 8-12 child designers, and therefore future work should further investigate and expand upon findings presented here in a larger study. In particular, it was not our research goal to explore differences among monitoring preferences based on children's gender or age, and our survey data would be insufficient to show significant results. Nevertheless, the emergent trends we noted would benefit from exploration in a larger study. Future work should also consider ways children's preferences may be influenced by cultural expectations and the preferences of children with more varied degrees of technical familiarity.

CONCLUSION

Our work envisioned new futures for and presents new perspectives on mobile monitoring technologies by working with children as co-designers. Results showed that, while children acknowledged mobile safety needs and accepted certain parental controls, they preferred technologies that emphasized restriction over monitoring, taught risk coping, promoted parent-child communication, and automated interactions. The expanded understanding of children's desires for mobile monitoring technologies advances the goal of developing flexible tools that fit into family value systems. Our results benefit designers looking to develop parental mobile monitoring technologies in ways that children will both accept and can actively benefit from.

ACKNOWLEDGMENTS

We offer our sincere thanks to all of the child and adult design partners of the University of Maryland's Kidsteam.

REFERENCES

1. Monica Anderson. 2016. *Parents, Teens and Digital Monitoring*. Pew Research Center, Washington, DC. Retrieved June 22, 2017 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 SIGCHI Conference on Human Factors in Computing Systems* (CHI '16), 3895-3905.
3. Carol Barron. 2014. "I had no credit to ring you back": Children's strategies of negotiation and resistance to parental surveillance via mobile phones. *Surveillance & Society* 12, 3: 401–413.
4. Lindsay Blackwell, Emma Gardiner, and Sarita Schoenebeck. 2016. Managing Expectations: Technology Tensions among Parents and Teens. In *Proceedings of the ACM Conference on Computer-Supported Cooperative Work & Social Computing* (CSCW), 1390-1401. https://doi.org/10.1145/2818048.2819928
5. Alicia Blum-Ross and Sonia Livingstone. 2016. *Families and screen time: Current advice and emerging research*. Media Policy Project, London School of Economics and Political Science, London.
6. Emma Bond. 2010. Managing mobile relationships: Children's perceptions of the impact of the mobile phone on relationships in their everyday lives. *Childhood* 17, 4: 514–529. https://doi.org/10.1177/0907568210364421
7. Leanne Bowler, Eleanor Mattern, and Cory Knobel. 2014. Developing Design Interventions for Cyberbullying: A Narrative-Based Participatory Approach. In *iConference 2014 Proceedings. Breaking Down Walls: Culture, Context, Computing*.
8. Dimitri A Christakis. 2010. Internet addiction: A 21stcentury epidemic? *BMC Medicine* 8, 1. https://doi.org/10.1186/1741-7015-8-61
9. Common Sense Media. 2017. *The Common Sense Census: Media Use By Kids Age Zero to Eight.* Common Sense Media, San Francisco, CA. Retrieved from https://www.commonsensemedia.org/research/
10. 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* (SOUPS), 19–35.
11. 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
12. Neil Davidson, John Vines, Tom Bartindale, Selina Sutton, David Green, Rob Comber, Madeline Balaam, Patrick Olivier, and Gillian Vance. 2017. Supporting Self-Care of Adolescents with Nut Allergy Through Video and Mobile Educational Tools. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '17), 1078–1092. https://doi.org/10.1145/3025453.3025680
13. Kerry Devitt and Debi Roker. 2009. The Role of Mobile Phones in Family Communication. *Children & Society* 23, 3: 189–202. https://doi.org/10.1111/j.1099-0860.2008.00166.x
14. Ditch the Label. 2017. *The Annual Bullying Survey 2017*.
15. Allison Druin. 1999. Cooperative Inquiry: Developing new technologies for children with children. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (CHI), 592–599. https://doi.org/10.1145/302979.303166
16. Andrea Düerager and Sonia Livingstone. 2012. *How can parents support children's internet safety?* London School of Economics, London, UK.
17. Jerry Alan Fails, Mona Leigh Guha, and Allison Druin. 2012. Methods and Techniques for Involving Children in the Design of New Technology for Children. *Foundations and Trends in Human–Computer Interaction* 6, 2: 85–166. https://doi.org/10.1561/1100000018
18. Trine Fotel and Thyra Uth Thomsen. 2003. The Surveillance of Children's Mobility. *Surveillance & Society* 1, 4. Retrieved from https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3335
19. Jennifer Golbeck and Matthew Louis Mauriello. 2016. User Perception of Facebook App Data Access: A Comparison of Methods and Privacy Concerns. *Future Internet* 8, 2: 9. https://doi.org/10.3390/fi8020009
20. Mona Leigh Guha, Allison Druin, and Jerry Alan Fails. 2013. Cooperative Inquiry Revisited: Reflections of the past and guidelines for the future of intergenerational co-design. *International Journal of Child-Computer Interaction* 1, 1: 14–23. https://doi.org/10.1016/j.ijcci.2012.08.003
21. 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 Conference on Interaction Design and Children* (IDC '16), 367–378. https://doi.org/10.1145/2930674.2930680
22. 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 Conference on Computer-Supported Cooperative Work & Social Computing* (CSCW '16), 1376–1389. https://doi.org/10.1145/2818048.2819940

23. Alex Kuhn, Brenna McNally, Shannon Schmoll, Clara Cahill, Wan-Tzu Lo, Chris Quintana, and Ibrahim Delen. 2012. How students find, evaluate and utilize peer-collected annotated multimedia data in science inquiry with zydeco. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI'12), 3061-3070. https://doi.org/10.1145/2207676.2208719
24. Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara Clegg, and Jessica Vitak. 2017. 'No Telling Passcodes Out Because They're Private': Understanding Children's Mental Models of Privacy and Security Online. In *Proceedings of the ACM Conference on Computer-Supported Cooperative Work* (CSCW'17*)*. https://doi.org/ 10.1145/3134699
25. Sonia Livingstone and Ellen J. Helsper. 2008. Parental Mediation of Children's Internet Use. *Journal of Broadcasting & Electronic Media* 52, 4: 581–599. https://doi.org/10.1080/08838150802437396
26. Melissa Mazmanian and Simone Lanette. 2017. "Okay, One More Episode": An Ethnography of Parenting in the Digital Age. In *Proceedings of the Conference on Computer Supported Cooperative Work and Social Computing* (CSCW '17), 2273–2286. https://doi.org/10.1145/2998181.2998218
27. Anne-Marie Oostveen, Asimina Vasalou, Peter van den Besselaar, and Ian Brown. 2014. Child Location Tracking in the US and the UK: Same Technology, Different Social Implications. *Surveillance & Society* 12, 4: 581–593.
28. Jennifer A. Rode. 2009. Digital Parenting: Designing Children's Safety. 244–251.
29. Tonya Rooney. 2010. Trusting Children: How do surveillance technologies alter a child's experience of trust, risk and responsibility? *Surveillance & Society* 7, 3/4: 344–355.
30. Kiley Sobel, Arpita Bhattacharya, Alexis Hiniker, Jin Ha Lee, Julie A. Kientz, and Jason C. Yip. 2017. It wasn't really about the Pokémon: Parents' Perspectives on a Location-Based Mobile Game. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (CHI), 1483–1496. https://doi.org/10.1145/3025453.3025761
31. Anthony J. Viera and Joanne M. Garrett. 2005. Understanding interobserver agreement: the kappa statistic. *Family Medicine* 37, 5: 360–363.
32. Greg Walsh, Elizabeth Foss, Jason Yip, and Allison Druin. 2013. FACIT PD: A Framework for Analysis and Creation of Intergenerational Techniques for Participatory Design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2893–2902. https://doi.org/10.1145/2470654.2481400
33. Barbara J. Wilson. 2008. Media and Children's Aggression, Fear, and Altruism. *The Future of Children* 18, 1: 87–118. https://doi.org/10.1353/foc.0.0005
34. Pamela Wisniewski, Arup Kumar Ghosh, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2017. Parental Control vs. Teen Self-Regulation: Is There a Middle Ground for Mobile Online Safety? In *Proceedings of the ACM Conference on Computer Supported Cooperative Work and Social Computing* (CSCW '17), 51–69. https://doi.org/10.1145/2998181.2998352
35. Pamela Wisniewski, Haiyan Jia, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2015. "Preventative" vs. "Reactive": How Parental Mediation Influences Teens' Social Media Privacy Behaviors. In *Proceedings of the ACM Conference on Computer Supported Cooperative Work & Social Computing* (CSCW '15), 302–316. https://doi.org/10.1145/2675133.2675293
36. Pamela Wisniewski, Heng Xu, Mary Beth Rosson, 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 ACM Conference on Computer Supported Cooperative Work and Social Computing* (CSCW '17), 523–540. https://doi.org/10.1145/2998181.2998236
37. Maxine Wolfe. 1978. Childhood and Privacy. In *Children and the Environment*, Irwin Altman and Joachim F. Wohlwill (eds.). Plenum Press, New York, NY, 175–222.
38. Sarita Yardi and Amy Bruckman. 2011. Social and Technical Challenges in Parenting Teens' Social Media Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '11), 3237–3246. https://doi.org/10.1145/1978942.1979422
39. Leah Zhang-Kennedy, Christine Mekhail, Yomna Abdelaziz, and Sonia Chiasson. 2016. From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats. In *Proceedings of the Conference on Interaction Design and Children* (IDC '16), 388–399. https://doi.org/10.1145/2930674.2930716
40. Kids & Tech: The Evolution of Today's Digital Natives | Influence Central. Retrieved September 4, 2017 from http://influence-central.com/kids-tech-the-evolution-of-todays-digital-natives/
41. Cell Phone Monitoring for Iphone and Android Smartphones and Tablets. *TeenSafe*. Retrieved September 4, 2017 from https://www.teensafe.com/