Article

Journal of Adolescent Research
1–29
© The Author(s) 2019
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/0743558419884692
journals.sagepub.com/home/jar
SAGE

Beyond Parental Control: Designing Adolescent Online Safety Apps Using Value Sensitive Design

Karla Badillo-Urquiola[1], Chhaya Chouhan[1], Stevie Chancellor[2], Munmun De Choudhary[2], and Pamela Wisniewski[1]

Abstract

Parental control applications are designed to help parents monitor their teens and protect them from online risks. Generally, parents are considered the primary stakeholders for these apps; therefore, the apps often emphasize increased parental control through restriction and monitoring. By taking a developmental perspective and a Value Sensitive Design approach, we explore the possibility of designing more youth-centric online safety features. We asked 39 undergraduate students in the United States to create design charrettes of parental control apps that would better represent teens as stakeholders. As emerging adults, students discussed the value tensions between teens and parents and designed features to reduce and balance these tensions. While they emphasized safety, the students also designed to improve parent-teen communication, teen autonomy and privacy, and parental support. Our research contributes to the adolescent online safety literature by presenting design ideas from emerging adults that depart from the traditional paradigm of parental control. We also make a pedagogical contribution by leveraging design charrettes as a classroom tool for engaging

[1]University of Central Florida, Orlando, USA
[2]Georgia Institute of Technology, Atlanta, USA

Corresponding Author:
Karla Badillo-Urquiola, College of Engineering and Computer Science, University of Central Florida, Orlando, FL 32816, USA.
Email: kcurquiola10@knights.ucf.edu

college students in the design of youth-centered apps. We discuss why features that support parent-teen cooperation, teen privacy, and autonomy may be more developmentally appropriate for adolescents than existing parental control app designs.

Keywords
adolescent online safety, emerging adulthood, parental control apps, privacy, value sensitive design

According to Pew Research, 95% of teens have access to a smartphone device and 45% of teens say they are online almost constantly (Anderson & Jiang, 2018). Smartphones allow teens to have constant access to the Internet and social media apps, which may increase online risk exposure to harassment, information breaches, and involuntary/unwanted sexual, emotionally distressful, and toxic content (Mitchell, Jones, Finkelhor, & Wolak, 2014). Parental control applications ("apps") are one approach that parents use to monitor the risks of online content for teens. These apps allow parents to block, filter, or monitor their teens' online activities through their smartphones. However, research on the use of these apps has shown mixed results in terms of both effectiveness and how they affect parent-teen relationships. For instance, Davis and Koepke (2016) found that a stronger parent-teen relationship helps protect teens from online risks more effectively than parental restrictions. Ghosh, Badillo-Urquiola, Guha, LaViola, and Wisniewski (2018) found that teens resented these apps because they are privacy invasive, overly restrictive, and harm trust between parents and teens.

We argue that existing parental control apps may inadequately support the developmental process of adolescents because apps do not balance the values and needs of parents with those of teens. In this article, our goal is to explore whether and how we can shift the design of parental control apps from overly restrictive, parent-focused safety strategies to a more balanced approach that respects the developmental needs of adolescents. One approach that can negotiate tensions in value conflicts between different stakeholders of a technology is Value Sensitive Design (VSD). VSD (Friedman, Kahn, & Borning, 2003) is a theoretically grounded approach traditionally used within the Human-Computer Interaction (HCI) research community to help identify and embed human values into systems design. To understand how to balance value tensions between parents and teens, we conducted an in-class design exercise with college students in the United States using VSD to facilitate design ideas for youth-centric parental control apps. We posed these research questions that guided this exploratory study:

Research Question 1 (RQ1): What values do college students believe should be embedded in the design of online safety apps for teens?
Research Question 2 (RQ2): What types of features would college students design for making parental control apps more representative of the needs of teens?
Research Question 3 (RQ3): How do these designs compare to the status quo of parental monitoring apps?

To answer these questions, we conducted an in-class design exercise with 10 groups of 39 undergraduate students taking a computing ethics course. Students created "VSD design charrettes," or sketches of parental control app features that focused on youth-centric values (as opposed to parent-centric values) for protecting teens from online risks. Using VSD as our theoretical lens, we used a grounded thematic approach to identify key values college students thought should be embedded within parental control apps for teens.

A key contribution of this work is merging concepts from the field of HCI with a developmental perspective of adolescence to improve the design of online safety tools for teens and parents. HCI is a multidisciplinary field that incorporates principles from computer science, psychology, and human-factors engineering to investigate how people use technologies and how design influences use (May, 2001). This work also contributes a pedagogical tool for engaging college students in the practice of applying user-centered design principles to conceptualize parental control apps that are more youth-centered. Therefore, educators and app designers will find practical significance in our work. By using VSD, we reflect on the value tensions between online safety and privacy as well as the tension between parental control and teen autonomy over teens' online and mobile activities. Finally, we provide psychologists, researchers, and app developers more youth-centric ideas for parental control apps that conceptualize parents and teens as joint stakeholders in adolescent online safety.

Literature Review

In this section, we describe the developmental characteristics of adolescence, summarize the literature in adolescent mobile online safety, and introduce VSD.

Developmental Characteristics of Adolescence

During adolescence, a teen begins to form their ego identity, focusing more on themselves as individuals, rather than as a part of their family unit

(Mayseless, Wiseman, & Hai, 1998; Youniss & Smollar, 1985). Teens begin to gain more independence and engage in more risk-taking behavior, a natural and necessary part of this process (Baumrind, 1987; Steinberg, 2004). As such, the relationship between parents and teens becomes increasingly complex; the authority of parents shifts from unilateral control to more cooperative interactions during adolescence (Youniss & Smollar, 1985). A teen's need for autonomy from their parents is directly related to their need for privacy and respect (Rossler, 2005). Yet, trust is also critical factor in an adolescent's relationship with their parents (Williams, 2003), where some level of monitoring and information disclosure from teens is necessary so that parents can trust their teen is safe from harm (Kerr, Stattin, & Trost, 1999). Given that adolescence is already a tumultuous stage of distancing from one's parents, seeking new social experiences, and taking more risks, in the next section, we discuss how the introduction of the Internet and mobile devices has made this transitional period even more complex for families.

Adolescent Mobile Online Safety and Privacy

Negotiating privacy expectations between teens and parents is a challenging problem (Petronio, 2010), especially as it relates to online safety, parental monitoring, and smartphone usage. For instance, Davis, Dinhopl, and Hiniker (2019) found that smartphones can negatively affect parent-teen relationships, creating tensions and disconnects between them. Blackwell, Gardiner, and Schoenebeck (2016) found that the "practical obscurity" (i.e., how information can be hidden from others) of children's mobile devices leads parents to underestimate the ways in which their children use smartphones and creates anxiety for parents, which may encourage them to use more restrictive parenting strategies. Mazmanian and Lanette's (2017) ethnography study of families found that parenting technologies that provide parents more visibility of their teens' online behaviors were often restrictive and inflexible to the digital practices of families.

In 2017, Wisniewski, Ghosh, Xu, Rosson, and Carroll (2017) feature analysis of 75 commercially available parental control apps confirmed that these apps cater to the needs of parents over teens. Most of the apps increased parental control through surveillance-based mechanisms (e.g., showing parents all text messages a teen sent or received) and features that restricted teen activities, such as web browsing, app use, and screen time. Thus, the researchers concluded that commercially available parental control technologies are incongruent with teens' developmental needs for autonomy from their parents, socialization, and an appropriate level of risk-seeking, which is necessary for helping teens develop coping skills to effectively manage online risks (Wisniewski et al., 2015; Wisniewski, Xu, Rosson, Perkins, & Carroll, 2016). Therefore, we explore how we might move away from parental control to more youth-centric designs that promote adolescent online safety.

Using the Lens of VSD

VSD is a theoretically grounded approach that seeks to systematically embed human values within the design process (Friedman et al., 2003). VSD is a tripartite methodology of conceptual, empirical, and technical investigations that can both reflectively identify and proactively embed values that are of moral importance into the design of systems (Friedman et al., 2003). Based on VSD, our article is considered a conceptual investigation, which allows us to ask questions such as, "who are the direct and indirect stakeholders affected by the design as hand?" and "what values are implicated?" (Friedman, Kahn, & Borning, 2006, p. 72). Previous research within teen mobile safety has used this tripartite approach for identifying key technical design challenges with teens and parents (Czeskis et al., 2010); through this lens, research found that safety, trust, and privacy were values that caused tension between parents and teens. Nouwen, Van Mechelen, and Zaman (2015) found that parents value involvement, in addition to safety and control. VSD is well-suited for the context of adolescent online safety because it allows designers (in this case, college students) to reflect on core values that can help design better safety measures for teens.

Method

In this section, we describe our participants, the pedagogical exercise completed by students, and our qualitative data analysis approach.

Participants

Students were enrolled in a computing ethics class required for computer science majors. It was an ideal setting for exploring value tensions in the design of parental control apps due to its focus on contemporary issues surrounding computing, ethics, and society. Our participants were senior-level, undergraduate college students (approximately 22-24 years old) at a large public Southeastern research university. This age range is indicative of the developmental stage of emerging adulthood (Arnett, 2000), which has been described as "the Age of feeling in-between," as individuals are no longer adolescents but are also not adults (Arnett, 2000, p. 14). Given their positionality, these students (as future designers and developers) offered a novel perspective on the value tensions between parents and teens. As the first generation of emerging adults (i.e., generation Z) who grew up having smartphones (Dimock, 2019) and as computer science majors, they were well-positioned to design meaningful and feasible app features with little guidance from the researchers. The course is taught as a mixed lecture-discussion class, where students actively work together. On the day of the design exercise, 39 out of 44 students attended class and 12 out of the 39 students were women. Students formed their groups of three to five students, 10 groups total for the exercise. Attendance was mandatory, though participation in the exercise was voluntary. The data for this exercise was collected during Spring 2018.

Procedure

The last author was invited to give a lecture to the students on the topic of adolescent online safety, privacy, and ethics. This talk included an introduction to the "privacy paradox" literature, which discusses how teens (13-17 years old) disclose personal information about themselves online, exposing them to serious online risks (Barnes, 2006). It also provided statistics from Pew Research (Pew Research Center, 2013) showing the frequency in which teens go online and use social media, as well as statistics from the Crimes Against Children Research Center (Mitchell et al., 2014; Wolak, Mitchell, & Finkelhor, 2006) on the prevalence in which teens encounter unwanted sexual solicitations, online harassment, and explicit content online. This introduction to the topic of adolescent online safety led into a class discussion, where the students were asked as follows: "*When it comes to privacy and ethics, what matters more? A teen's right to privacy or a parent's ethical responsibility to protect their teens from online risks?*" While we did not record the class discussion (as we did not anticipate converting this course activity into a research collaboration), students took stances on both sides of this debate. Some of the students even mentioned that their parents used parental control apps when they were teens.

Next, the students were introduced to VSD (Friedman et al., 2003) in the context of parental control apps. Based on the results from Wisniewski et al.'s (2017) feature analysis, the students were shown how most parental control apps currently focus on parental monitoring and restriction for keeping teens safe online. Based on the presentation describing the status quo of existing parental control apps as focused more on parent-centric needs, students were then asked to create "VSD design charrettes" (Spendlove, 2015) that focused more on youth-centric values. Specifically, we asked them to

> create a **VSD charrette** for parental control apps used to protect teens from online risks. Instead of the values currently being embedded within parental control apps, **choose new values** that are more representative of **teens as key**

> **stakeholders**. **Draw a mock-up** of a new app based on these teen-centric values. **Annotate** your drawing to explain how the app would work. **Take a picture** of your charrette and design.

We used a VSD conceptual approach design (Friedman et al., 2003) to ask students to redesign parental control apps by identifying key values that should be accounted for. Our conceptual approach directed students to thoughtfully consider who the direct and indirect stakeholders of their app would be and how might they be impacted by their designs (e.g., what are the benefits and harms of the app). We also asked the students to carefully consider whose values should be incorporated into the design and the trade-offs of competing values. From these discussions, students were then able to create their design charrettes.

The third author, who was the course's teaching assistant, facilitated group work in the class by answering student questions. As they designed their charrettes in class, students were invited to share their ideas and motivations behind their designs. They were also given the opportunity to iterate on their designs with their groups after class. Groups were asked to scan or take photos of their charrettes and submit their VSD charrettes within several days after class via an anonymized Dropbox folder. Students were told that their designs may be incorporated into future research and were invited to email the last author if they were interested in collaborating on a research project around their idea(s) in the future. At the time of the class exercise, we did not intend to analyze the design charrettes and publish this article.

After reviewing the ideas submitted by the college students, we were impressed by their quality and insights. We realized that college students, as emerging young adults, were uniquely positioned to empathize with the needs of both teens and parents in a way that served to balance key design tensions discussed during the class lecture. Therefore, we asked our Institutional Review Board (IRB) about conducting a retrospective, secondary data analysis. Our IRB made the determination this was "Non-Human subjects" research. Their rationale was that the data were collected in an educational setting that involved normal educational practices that were not likely to adversely impact students. Furthermore, the data were de-identified prior to analysis and could not be linked back to students. With this approval, we continued with our analysis.

Data Analyses

We analyzed 10 VSD design charrettes that were submitted by the students. The charrettes included low-fidelity visual representations of the designs (i.e., drawn mock-ups on paper), annotations, and textual explanations. We first conducted a grounded analysis (Braun & Clarke, 2006) of the design charrettes to identify each unique design feature (RQ2). We conceptually grouped the designs based on similar features and describe variations between the groups' designs. We then analyzed the charrettes to extract values that the students believed should be taken into consideration when developing future parental control technologies (RQ1). We incorporated both the explicitly stated values as well as the values that were implicitly implied by the designs in our analyses. Then, we grouped the unique features based on the primary value they supported. The first and second author worked together to code and conceptually group each of the features by the intended value.

Next, we used a deductive and inductive coding approach (Fereday & Muir-Cochrane, 2006) to map the features identified to the Teen Online Safety Strategies (TOSS) framework (Wisniewski et al., 2017). The TOSS framework is a theoretically derived conceptualization of the primary strategies used to keep teens safe online. In TOSS, online safety features are categorized under two dimensions: parental control and teen-self regulation. The three parental control strategies are as follows: (a) *monitoring*: through passive surveillance, (b) *restriction*: through rules and limitations imposed on technology use, and (c) *active mediation*: through talking to teens about technology use and their online experiences. The three teen-self regulation strategies are as follows: (a) *self-monitoring*: self-awareness and self-observation, (b) *impulse control*: suppressing short-term desires to prevent long-term consequences, and (c) *risk-coping*: managing online risky interactions after they occur. A fourth dimension that emerged in TOSS was *parent and teen education* about online safety.

We used this framework as the basis of our qualitative analysis to classify the students' design-based features (Table 2). Finally, we compare Wisniewski et al.'s (2017) empirical feature analysis of 75 existing parental control apps to the features extracted from the students' VSD design charrettes (Figure 2) to determine if our pedagogical exercise was helpful in shifting the balance from features heavily focused on parental control to those that supported parent-teen collaboration or teen self-regulation (RQ3). The first and second author met in-person and conducted their analyses together using an iterative, consensus-based approach. If they had disagreements or questions, they consulted the last author who helped them resolve conflicts and refine their analyses. We present the results of our qualitative analyses below.

Results

We first provide an overview of the features extracted from the design charrettes organized by the key values we identified within their designs. We then use the TOSS framework (Wisniewski et al., 2017) to compare our results to the status quo of parental control apps.

Identifying Values in Design Within the Parental Control Design Charrettes

In total, we identified 16 unique features from the 10 design charrettes. Of the 10 design charrettes, five groups designed their apps to be used by parents. Four groups designed their apps for both parents and teens. One group created an app for only teens. Figure 1 provides a few examples of the students' design charrettes.

We grouped similar features into categories based on the key value represented in design (see Table 1). In the sections below, we organize our results first by values in design, then by the unique features designed by each group (we refer to specific groups as G*x* where *x* is the group we are referring to). We present our results in descending order based on the frequency.

Safety features. One of the most prevalent values, present in eight of the 10 design charrettes, was protecting teens from online risks (i.e., safety). Students embedded this value in their design charrettes by incorporating features that supported parental alerts, risk detection, conversation previews, risk ratings, and flagging a friend. The most common safety feature designed was *parent alerts* (six groups) that would "show" or "send" parents notifications for threatening situations that the teen encountered online. For example, parental alerts notified parents instantly whenever a risk was detected in a teen's conversation or if the teen received a text message from an unknown number. The parental alert was meant to help parents quickly handle a risky situation and keep the teen safe from imminent harm.

To implement parental alerts, half (5) of the design charrettes leveraged automated *risk detection* to identify whether the teen was encountering online risks. For instance, G1 and G2 both designed apps which used "machine learning" to identify and flag risky conversations based on a set of keywords and/or the time of the day. Similarly, G10 suggested "advanced artificial intelligence to determine dangers in conversation." In contrast, G4 suggested the use of "image recognition" to detect risky images before a teen shared the image with others.

Three groups gave the parent a *conversation preview* with alerts, where parents were given a snapshot of the conversation that was flagged as risky. To some extent, this feature helped balance the value tensions between teen safety and privacy by giving parents low-level details of conversations only when content was identified as risky.

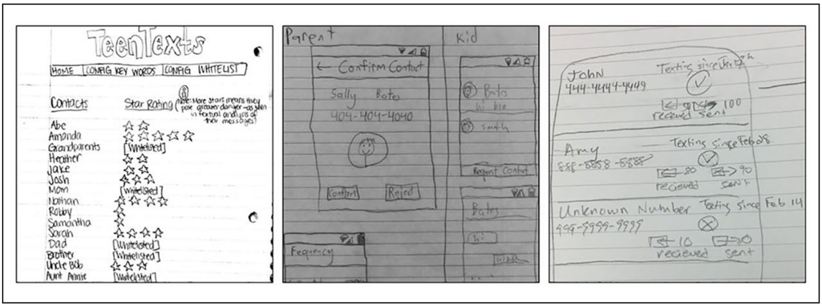

Figure 1. Examples of students' design charrettes: (a) risk rating (left, group 1), (b) whitelist (middle, group 8), and (c) conversation metadata (right, group 9).

Table 1. Value-Feature Mapping.

Values in design					
	Safety (8/10)	Parent-teen communication (7/10)	Teen autonomy (5/10)	Teen privacy (4/10)	Parent support and growth (1/10)
Unique features identified	Parental alert (G1, G2, G3, G5, G7 G10) Risk detection (G1, G2, G3, G4, G10) Conversation preview (G1, G2, G3) Risk rating (G1) Flag A friend (G9)	Whitelist (G1, G2, G7, G8, G9) Teen alert (G3, G10) Ask your child (G7, G9) Ask your parent (G8)	Parent-teen settings controls (G1, G3, G10) Teen account (G4, G8) Intelligent assistant (G4) Teen support services (G3)	Conversation metadata (G5, G8, G9, G10)	Parental support group (G6) Leaderboard (G6)

Note. This table presents the value-feature mapping. Each column heading represents a value, and below are the corresponding features that map to those values. Next to each feature, we indicate the groups that proposed them. The counts next to each value represent the total number of groups (out of 10) that designed a feature to support that value.

Other safety features included G1's *risk-ratings* (Figure 1a), which used "textual analysis" of messages to assign star-ratings to the people in the teen's contacts list based on the amount of risk detected in conversations with those individuals. The more stars a person had, the more dangerously they were perceived. G9 proposed a similar feature called *flag a friend*, where parents could manually flag (mark) a teen's contacts that they thought were suspicious or potentially threatening, so they could ask the teen about this "friend."

A key theme among these safety features was that they attempted to use either manual or automated approaches to detect online risks and notify parents, so parents could help mitigate these risks. Online risks were often identified within the context of a given conversation, but in some cases, risk was associated with a given context (e.g., time of day) or certain individuals (possibly based on conversations) who the teen interacted with via their mobile device.

Features for improving parent-teen communication. Seven groups designed features that attempted to improve parent-teen communication, rather than protecting the teen directly from online risks. Five groups designed a *whitelist* feature for parents, so that they could create a trusted contact list for whom their teen could interact without constant supervision. This feature helped alleviate tension between parents and teen by giving the teen some leeway to communicate with trusted friends and family. One group (Figure 1b) gave teens the ability to ask parents to "confirm" or "reject" a new contact based on the contact name, phone number, photo, and a preview of the initial messages within the conversation. This allowed parents and teens room to negotiate whether certain contacts were trusted or not, increasing their communication with one another.

Two groups designed apps with *teen alerts*. These groups decided that risk alerts should be sent to teens as well as parents. This feature helped teens understand what interactions triggered risk alerts and allowed them to know beforehand if they were about to be approached by their parents (or possibly get in trouble) about these risky interactions. One group also alerted teens if a parent changed any settings of the app. These teen alerts may help parents and teens form a mutual understanding of shared expectations about mobile phone use.

Two groups designed a communication feature for *asking the child*, which helps parents start a discussion with their teen. These discussions could include concerns parents had regarding certain people their teen interacted with that seemed suspicious. Instead of restricting the ability for the teen to communicate with potentially unsafe people, the feature gave teens and parents a shared communication channel for further discussion.

Similarly, G8 created an *ask your parent* feature to allow teens to start a conversation with their parents about individuals they want to interact with. This feature provides the opportunity for both parents and teens to communicate and negotiate limits.

Features to support teen autonomy. Five groups focused on developing features that provided some level of autonomy to the teen, so that they could observe and learn from their own actions. Three groups suggested shared *parent-teen settings controls*. For instance, G3 proposed that teens should be considered a part of the parental monitoring process, and the app should be more transparent for teens to observe how the parental monitoring is taking place. Therefore, they designed an app where both teens and parents could control the settings of the app. Parents could adjust the strictness of the parental control apps features using a slider. The strictness was meant to be flexible with respect to the teen's actions.

Two groups purposefully designed *teen accounts*, so the teen could have their own separate user interface apart from their parent. These accounts allow teens the opportunity to manage their own online behaviors. Even though the design prompt directed students to redesign a parental control app, one group created an account only for teens. They proposed an *intelligent assistant* that would use image recognition to warn teens before sharing risky images with others. Their design charrette mocked-up a conversation between a sexual predator and a teen, where the teen was asked to "show me the goods." The app would detect the inappropriate image, stop transmission, and ask the teen if they are sure they want to send it. This feature promotes autonomy because it gives the teen the agency to override the warning and send the sexually explicit image. In this case, G4 included automated risk detection for notifying the teens of their own risky behavior, rather than their parents. This helps teens be more responsible of their choices and consider the consequences of their actions.

One group suggested a trigger to provide *teen support services* to help the teen understand the consequences of their actions. G3 proposed that whenever a teen triggered an alert to the parents, resources would be provided to help the teen understand the consequences of their actions. This feature provided immediate resources to the teen beyond expecting their parents to address the situation with them upon being alerted.

Privacy-preserving features for teens. Four groups sought to create a balance between safety and privacy by giving parents a window into their teens' online activities but not making this window completely transparent. They did this by only giving parents *conversation metadata*, rather than the actual content of their teens' messages. Conversation metadata included information like who the teen was talking to (e.g., contact name, screen name, or number), number of messages sent or received, at what time they talked, the duration of the conversation, and how many messages were exchanged. Because the metadata did not contain details of the conversation itself, it helped keep the teens' data private while still providing essential information to parents. G8 argued that it was also important to maintain the privacy of the teen's contacts as parental control apps were not only intrusive to the teen's personal privacy, but they also invade the privacy of others like the teens' friends. Figure 1c provides an example of a feature that leveraged conversational metadata, such as name, number, how long the teen had been texting with the individual, and number of messages sent and received.

Features for parental support and growth. One group designed an app that encouraged parents' personal growth through support and competition. G6 designed a community-based, parental monitoring app which would foster communication among parents to provide support and teach them how to improve their parenting. Parents would have access to a *parental support group*, where they could discuss their concerns with other parents to learn how to deal with certain situations/scenarios. They could share their experiences, tips/techniques, and help each other take better care of their teens. This group designed a *leaderboard*, where smaller groups of parents could compete, and the winner would be awarded the title of "Best Parent." The group explained, "*Parents ratings [were] based on parenting success*." Parents would keep track of good and bad behaviors exhibited by their teens, learn from other parents in the community by "*discuss[ing] with other parents how to handle [these] scenarios.*"

Overall, the groups designed features that kept teens safe by detecting online risks, so that parents could intervene, while affording teens more privacy over their online interactions. Instead of increasing parental control through restrictive features, the students emphasized features that enhanced parent-teen communication and build trust. The students also designed features for teens that promoted their autonomy and for parents to give them support and teach them how to manage their teens' risk-seeking behaviors more effectively. Next, we map these features to the TOSS framework.

Applying the TOSS Framework to the Design Charrette Features

Out of 16 features that were designed by the students to protect teens from online risks, most supported parental control strategies (11/16), and seven features supported teen self-regulation. Two features provided educational support to parents. Table 2 summarizes the mapping between the students' features and the TOSS framework, which we discuss below.

Parental control. In the parental control category (see Table 2), most features supported parental monitoring (4/11) and restriction (4/11); only two features supported education and one active mediation. We provide details about the features that supported parental control below.

Monitoring. Monitoring was one of the most observed TOSS dimensions in the students' design charrettes. Included in this category were risk detection, parental alerts, conversation metadata, and conversation preview.

Table 2. TOSS Mapping Based on Features Designed by Students.

Parental control (N = 11 features)				Teen self-regulation (N = 7 features)			
Monitoring (N = 4)	Restriction (N = 4)	Active mediation (N = 1)	Education (N = 2)	Self-monitoring (N = 3)	Impulse control (N = 2)	Risk-coping (N = 2)	Education (N = 0)
Risk detection (G1, G2, G3, G10) Parental alert (G1, G2, G3, G5, G7, G10) Conversation metadata (G5, G8, G9, G10) Conversation preview (G1, G2, G3)	Whitelist (G1, G2, G7, G8, G9) Parent-teen settings control (G1, G3) Risk rating (G1) Flag a friend (G9)	Ask your child (G7, G9)	Parental support group (G6) Leaderboard (G6)	Risk detection (G4) Teen alert (G3, G10) Teen account (G4, G8)	Intelligent assistant (G4) Parent-teen settings control (G3, G10)	Ask your parent (G8) Teen support services (G3)	N/A

Note. This table provides the TOSS mappings based on the features designed by students. Column headings represent the TOSS dimensions for parental control and teen self-regulation. Below are the corresponding features that represent each strategy and the groups that proposed them. The counts represent the number of features (out of 11 for parental control and out of 7 for teen self-regulation) that support each TOSS strategy. TOSS = Teen Online Safety Strategies.

Whenever a risk is detected, parental alerts provided the capability for parents to get notified. Although parents may not be continuously monitoring their child, they are providing direct oversight through the app by monitoring their child's activities when a risk is detected. Conversation metadata and preview are features that help parents keep track of what their teens are doing. The key novelty in the students' designs, compared with existing apps, is that the students afforded teens more privacy by abstracting and aggregating this information and only giving parents information when a risk was detected, rather than giving parents low-level details about a teen's online interactions (e.g., actual conversations, browser history).

Restriction. Four design features allowed parents to restrict certain teen activities to protect teens from online risks. This included the whitelist feature (which had an analogous "blacklist" option), where teens could only talk to people who have previously been approved by their parents. G9 provided the option to flag a friend, where if the parents mark a child's contact as risky, it restricts the teen from engaging in conversation with that contact. Similarly, in G1's risk-rating feature, contacts are given a star rating based on the prevalence of risk associated with them. Finally, G10's parent-teen settings control allows the parent to adjust the strictness of the parental control features to restrict the teen's online activities. A key theme among restrictive features is that they mostly focused on restrict *with whom* teens could interact, rather than what they could do from their phones. Even though these features gave parents the ability to restrict teens from communicating with unsafe people, teens had some say in the decision.

Active mediation. There was one feature (ask your child) that supported active mediation from parent to child. G7 and G9 suggested having an *ask your child* feature where parents could initiate discussions with their teen about their activities. For example, parents and their teens could discuss a teen's new friend or contact, with the goal of promoting healthy communication between parents and teens.

Parental education. One group identified two educational features for parents, which entailed parental support groups and a leaderboard. These features could help educate parents on how to handle certain situations with their teens. Parents could discuss similar scenarios with other parents and learn from them. The leaderboard could help parents be more aware of their teens' needs, facilitating healthier relationships with their teens and improving trust.

Teen self-regulation. Seven features supported teen self-regulation strategies. Approximately half of the features supported self-monitoring (3/7), while two supported impulse control, two risk-coping, and no feature supported education for teens. Table 2 provides a summary of this mapping. Some features were double coded for both parent and teen strategies based on the intent of each group. For example, four groups designed risk detection features for parents (i.e., parental monitoring), while G4 designed their risk detection feature for teens (i.e., self-monitoring). The groups are listed in the table adjacent to each feature. We describe the features in relation to each teen self-regulation strategy below.

Self-monitoring. Three features supported teen self-monitoring through risk detection, teen alerts, and teen accounts. G4 used risk detection to give teens an opportunity to rethink whether they really wanted to send an explicit or otherwise inappropriate photo to one of their contacts. Other groups chose to send risk alerts to teens, as well as parents, which could raise their level of self-awareness when an alert was triggered. Teens also receive an alert when parental app settings were changed. These features for teen self-monitoring gave teens a stronger sense of personal agency over their online behaviors and the use of the parental monitoring app. Instead of the app only being used by parents, teens could login to the app, and see their activities and whether any risks were detected. Unlike many existing parental control apps that covertly monitor teens, these apps were more transparent and made teens joint users along with parents.

Impulse control. Two features promoted impulse control to help teens mitigate online risks on their own. G4 used an intelligent assistant, which prompted a warning to the teen asking if they were sure that they wanted to share a risky image. By first raising risk awareness, then explicitly asking a teen to reconsider their decision, this feature encouraged teens to think about the long-term consequences of their short-term actions. It places the responsibility of their decisions on themselves, rather than their parents. Another feature that promoted impulse control was the teen control settings, allowing teens the opportunity to change settings of the parental control app (e.g., setting safe locations). These settings gave teens responsibility to decide the boundaries in which they could be considered safe without the need for parental supervision. By giving teens the autonomy to make some decisions about online safety and risks, these features provided the space to exercise good judgment and self-control.

Risk-coping. While most features promoted strategies for helping teens prevent negative events, two features were designed to support strategies for helping teens overcome the effects of such an event once it occurred. G8

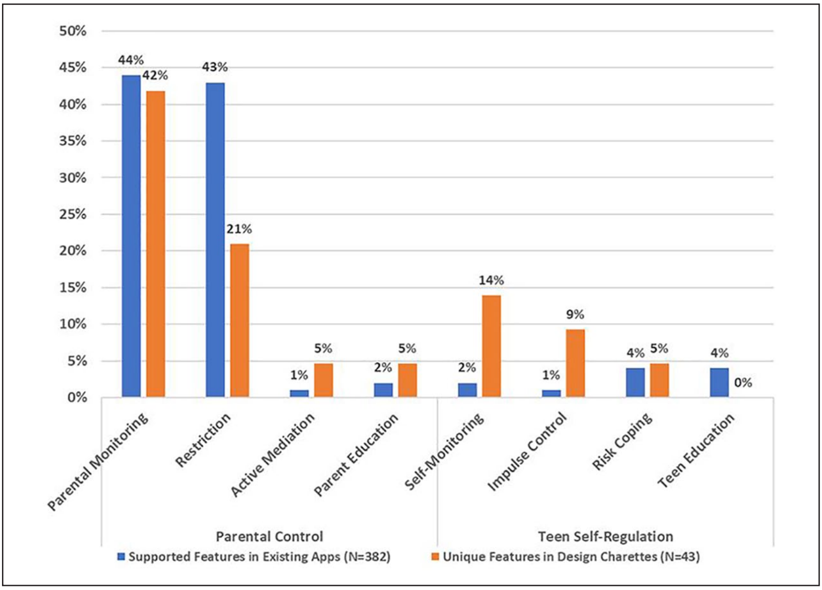

Figure 2. A comparison of existing parental control apps with students' design charrettes based on the TOSS framework.
Note. TOSS = Teen Online Safety Strategies.

created an ask your parent feature, which gave the teen an invitation to reach out to their parent for help. This feature could also be used to ask the parent to evaluate the trustworthiness of a new contact. G3 designed a teen support service feature, which provided teens external resources to help them after a risk event was detected. In this way, the feature acted to provide real-time assistance when a risky situation might be present. These features provided teens with support for advice-seeking and acquiring help at the time they might find it most valuable.

Comparing Students' Designs to the Status Quo of Parental Control Apps

In their paper, Wisniewski et al. (2017) found that the majority of features in the 75 apps they analyzed supported parental control (89%), while only 11% of the features supported teen self-regulation. Figure 2 provides a comparison between Wisniewski et al.'s (2017) empirical feature analysis of existing parental control apps (left) to the features we extracted from the students'

VSD design charrettes (right). Wisniewski et al.'s original analysis identified 382 instances of app features in the 75 apps, while ours identified 43 instances of app features within the 10 design charrettes. We standardized the graph for meaningful comparisons between these two analyses.

As shown in Figure 2, students still predominantly designed features for parental monitoring (42% of features in the design charrettes compared to 44% of features for existing parental control apps, respectively), but they designed considerably fewer features that supported parental restriction (21% vs. 43%). The shift toward more teen-centric features persists across the remainder categories in the graph. Comparatively, students designed more features for active mediation and parental education than what Wisniewski et al. found to be the status quo in existing parental control apps. Students also created more features for teen self-monitoring, impulse control, and risk-coping. However, they did not design features geared toward teen education about online safety. Overall, we saw a considerable shift toward more youth-centric designs; yet, we also acknowledge that the imbalance of parent features over features designed for teens. We discuss the implications of these findings in more detail in our discussion.

Discussion

Our research represents an important first step toward a more balanced approach to designing adolescent online safety apps. Overall, the college students designed for safety, parent-teen communication, teen autonomy and privacy, and parental support. While moving away from restrictive parenting practices, they still emphasized parental monitoring over teen self-regulation to prevent and mitigate online risks. We reflect on our results and propose design recommendations for parental control apps to better negotiate parental control and teen self-regulation.

Embedding Teen-centered Values in the Design of Parental Control Apps (RQ1)

We asked college students what values they felt were important to embed in the design of parental control apps when thinking about teens as potential end users. Safety emerged as the most prominent value in design, which was expected given the topic of the design prompt (i.e., adolescent online safety). Many of the parental monitoring features were designed for risk prevention, but other features, such as the "teen support services" or "intelligent assistant" for the teen promoted risk-coping and impulse control through increased self-awareness, respectively. Ultimately, these features moved toward promoting teen self-regulation. Similar to how Hiniker, Lee, Sobel, and Choe (2017) developed a tablet-based application that taught younger children to intentionally plan out their media use to encourage self-regulatory behaviors, we also encourage future researchers and designers to focus on more youth-centric approaches for adolescent online safety design that go beyond risk prevention and mitigation to teach teens how to effectively manage online risks.

The college students also placed great value on facilitating parent-teen communication to promote safety and balance the needs of two very different stakeholders. From a developmental perspective, this design pattern made sense. As teens mature, they seek more cooperative decision-making with their parents, rather than being subjected to unilateral authority (Youniss & Smollar, 1985). In other words, they want to be part of the decision-making process and not just told what they can and cannot do. Therefore, providing means for parents and teens to communicate through the apps may afford opportunities to negotiate boundaries, resolve conflict, and form shared expectations between parents and teens. Teen autonomy and privacy were also prominent values within the students' designs. Even though the students stayed mostly within the guidelines of the design prompt—to redesign existing parental control apps—they included features for parental monitoring that were more respectful of a teens' privacy (e.g., conversation previews, conversation metadata) by using machine learning as an automated approach to filter the data shared with parents. Overall, the students designed considerably fewer features for parental restriction than what exists in commercially available parental control apps. The students designed features to build stronger parent-teen relationships instead of increased parental control. Based on the research, such features may be more effective in helping teens navigate risk more effectively than the alternative of the status quo. Finally, many of the design charrettes included automated risk detection to help parents protect their teens from online risks; however, risk detection was also used for providing teens more privacy and autonomy from their parents. This demonstrated how college students tried to balance value tensions (i.e., teen safety, privacy, and autonomy) and their desire to be cognizant of the needs of both parents and teens. Overall, designing for safety, parent-teen communication, teen autonomy and privacy, and parental support and growth are more positive youth-centric family values than designing solely for parental control. Yet, how we embed these values within the design of adolescent online safety apps deserves additional scrutiny.

Implications for the Design of Parental Control App Features (RQ2)

In addition to leveraging the insights from the students' designs, we use a developmental perspective of adolescent online safety to inform our design recommendations.

By leveraging what is known about adolescent development, we can significantly improve the design of adolescent online safety apps. Following the college students' lead, designing apps that support teen self-regulation and parent-teen communication, rather than parental control, could help teens develop a stronger self-efficacy for protecting themselves online and making better decisions as they experiment with some level of online risk. Jia, Wisniewski, Xu, Rosson, and Carroll (2015) call this approach a "risk as a learning process" model for allowing teens to engage with technology, so that it can shape their online information privacy behaviors and teach them how to engage with others via social media in a safer way. One takeaway from the student designs is that parental control apps could be designed to include teens. Providing teens with their own interface might increase ownership, awareness, and buy-in (Hiniker, Schoenebeck, & Kientz, 2016; Ko, Choi, Yang, Lee, & Lee, 2015). At minimum, parental control apps should be designed to be transparent to the teen in contrast with existing apps that are often opaque. This approach would help teens use the information from the app to increase their own self-awareness, improve their impulse control, more effectively cope with online risks, and understand that the intent of the app is to help actively engage their parents for help, not to spy on them. G4's idea about using automated risk detection to help teens decode and reflect on their own risk behavior (e.g., sending a sexually explicit image) was a good example of helping teens to be better digital citizens (James, Weinstein, & Mendoza, 2019), rather than trying to police them.

Similarly, we recommend more features that leverage context-aware computing (e.g., being able to react in real time to an individual's changing context [Schilit, Adams, & Want, 1994]), combined with validated approaches from educational psychology to teach teens how to keep themselves safer online. For example, Havighurst's (1953) book on *Human Development and Education* emphasizes the importance of "teachable moments." He explains that a developmental task is one where it must be learned at the right time, so that learning can be most effective. For example, raising the risk awareness of teens in the context of a risky interaction (e.g., taking and sending an explicit photo) may be more effective than using generic warnings about appropriate sharing outside the context of that risky interaction.

Finally, teens should be given the ability to negotiate limits and rules with their parents. For example, customizable settings shared by the parent and teen could aid in boundary setting. In addition, settings could be designed to support the developmental changes and differences between younger teens (ages 13-14 years) and older teens (ages 16-17 years). While such transitional customization may prove to be more complex than G10's slider, it is worth exploring how an app could adapt and grow with the teen as they become more mature.

Moving Beyond the Status Quo of Parental Control for Adolescent Online Safety (RQ3)

In our study, the pedagogical exercise of having emerging adults create VSD design charrettes was successful in attempting to shift the design of parental control apps toward more youth-centric designs for teens. The students balanced different stakeholders (i.e., parents and teens) and value tensions that recognized parents not just as authority figures, but as advisors (Youniss & Smollar, 1985). In contrast, McNally et al. (2018) conducted a participatory design study with children (ages 7-12 years) and asked them to redesign an existing parental control app. The children designed for parental control and restriction, whereas the designs from emerging adults were much less authoritarian in nature. It would be valuable to test whether teens value freedom and parents more control with a study that involves teens and parents as designers.

After asking students to create design charrettes of parental control apps that were more representative of teen values, we saw a shift in their designs from the status quo (Figure 2). However, students still developed a limited number of features intended primarily for teens and focused heavily on less privacy invasive parental monitoring features. As such, we would like to highlight important methodological design implications for HCI researchers who leverage VSD methods—it is difficult to get people to design against the status quo—Khovanskaya et al. (2018) explains that rarely do we explore possibilities that go beyond societal norms to innovate technologies that go beyond (or even against) the status quo. Therefore, it is important to work deliberately to find opportunities that can give new perspectives to change. Khovanskaya et al. (2018) suggest a series of questions for researchers to use during the design process; these include the following: (a) “What is the status quo, and what needs to be changed?” (b) “What are the limits of design?” (c) “Who disagrees” or “who gives permission?” and (d) “What’s at stake?” (p. 4). We suggest that such questions should be asked when trying to reconceptualize adolescent online safety apps in a way that is developmentally beneficial to adolescents as we strive to keep them safe online. Next, we discuss the limitations of our approach and suggest ways to overcome these limitations and areas of future research that based our lessons learned.

Limitations and Future Work

We conducted a retrospective analysis of design charrettes created by college students as an initial and exploratory way to move away from the status quo of online safety tools that overly emphasize parental control. In retrospect, there are some study design decisions that we would have made differently. For instance, we realized that using the term "parental control app" within the design prompt could have inherently pushed participants to design for parents and for control. It may have been difficult for the students to creatively consider and design novel solutions beyond the traditional boundaries placed by parental control apps. Instead, we would have asked them to design an app for adolescent online safety or use more neutral terminology. We also acknowledge that the invited lecture prior to the design exercise could have influenced the students' designs, limiting their creativity. In addition, we did not perform a systematic evaluation of whether the exercise changed the attitudes, beliefs, or knowledge level of the students in terms of their perspectives of the design of parental control apps, nor how to generally apply VSD principles to balance tensions in design.

To overcome these limitations, we propose that future studies or classroom exercises first give students a pre-assessment, then design activities that are more open-ended, prior to introducing them to existing research on the topic. After the initial designs are submitted and students are oriented to the research, then they could be given the opportunity to iterate on their designs more intentionally given the goal of the design exercise. This would reduce potential bias and help students be more intentional about their design choices. Then, a post-survey could be used to assess whether the exercise helped shift the students' thinking and teach them concepts about user-centered design processes. Taking these steps would help address the question of whether students' designs were significantly affected by being in a computing ethics course or being introduced to the TOSS framework prior to participating in the design exercise.

Another limitation is that our sample was biased toward male computer science students. On one hand, male computer science students are the most likely demographic to develop future online safety apps. Therefore, this exercise helped us obtain useful insights from possible future designers and developers on how they would redesign online safety apps to incorporate more youth-centric values. It also helped us explore the practicality of using VSD design charrettes as a pedagogical tool to get students to consider and balance value tensions in design. On the other hand, we recognize the need for larger, more diverse perspectives when it comes to designing developmentally appropriate online safety tools for adolescents.

Furthermore, while we can present the design ideas created by college students, we cannot confirm they are good. In some cases, we can draw from existing research (Andrade, Mizoguchi, & Isotani, 2016) to ascertain that some of the design ideas were problematic (e.g., leaderboard ranking parents), while others present technical challenges. The user-centered design process requires multiple iterations to get a specific design pattern correct before implementation. Instead of focusing on the quality or technical feasibility of the designs, our intent was to focus on the values in designs and the higher-order ideas behind the designs in our analyses.

Given the developmental transition from childhood, adolescence, emerging adulthood, to becoming adults and/or parents, the differing perspectives, and particularly the differing values, of these user groups offers useful insights for how to carefully balance tensions and user needs that arise at different life stages. Yet, working directly with teens and parents is a logical and necessary next step. To build upon our findings, we recommend conducting participatory design studies (Fails, Guha, & Druin, 2013) with teens and parents as joint stakeholders in apps designed to promote the online safety of adolescents. It would be useful to see whether and how teens and parents would negotiate and resolve their own value tensions in the design of online safety apps. As a second step, teens and parents could evaluate the design proposed by the emerging adults. Table 3 summarizes parent and teen features suggested by the college students with potential research questions that could be used to help shape the study design. Furthermore, it would be worthwhile to work directly with teens, rather than including parents, to design online safety features that focus more on youth empowerment and teen self-regulation.

Finally, future research ought to explore how the design of adolescent online safety apps needs to change with the developmental needs of teens as they progress from early adolescence, mid-adolescence, late adolescence, to emerging adulthood. For example, how might we account for the tensions between parental control and teen autonomy differently—for when a teen (or younger child) is first given a smartphone, to when a teen transitions from middle school to high school, to finally when a teen becomes an emerging adult, similar to the college students whose designs we presented in this article. By taking a developmental approach to understanding the unique needs of teens during each of these transitional periods, we may be able to take a step toward designing new online safety tools that are beneficial to teens across the adolescent lifespan. To this end, we strongly encourage future endeavors that meaningfully merge human-centered design principles with knowledge in adolescent development to train future computer scientists how to build youth-centric technologies that are well-suited for teens.

Conclusion

In this article, we integrate a developmental perspective on adolescence with a human-centered approach to design to re-envision parental control apps

Table 3. Parent and Teen Features Designed by the Students.

New app features	Potential research questions
1. Risk detection with parent/teen alerts: Keywords are identified in a message sent to the teen and a notice with metadata or a preview of the conversation is sent to the parent and teen.	1. When detecting online risks, what risks are most salient, and what thresholds should be used based on the age and maturity of the teen?
2. Parent/teen user interface: Both parent and teen have a personal account and access to the app.	2. What features facilitate cooperation between parents and teens, rather than creating conflict?
3. Whitelist: Parents and teens will be able to assign a risk rating to contacts or flag contacts they feel may be dangerous.	3. How do parents and teens evaluate whether a new contact is safe or unsafe?
4. Ask your parent/teen: This feature prompts a conversation between the parent and teen to increase communication between them.	4. How could this feature be designed in a way that reduces parental judgment and encourages open and honest conversations?
5. Customizable settings: This allows for settings to be configured appropriately based on the teen's developmental growth.	5. How can we make online safety apps adapt to the developmental needs of teens as they transition from teens to emerging adults?
6. Intelligent assistant: Teens are warned before sharing a risky image or message with others.	6. What are the most effective ways to design behavior nudges that a teen will find useful?
7. Parent/teen support services: support groups for parents to talk about parenting practices and teens to talk about online safety strategies.	7. When designing for support, how can we mitigate the possibility of bad actors, unsolicited advice, or unhelpful commentary?

that are more youth-centric. In doing this, we make an empirical contribution to the domains of HCI and adolescent online safety research. We also make a pedagogical contribution by presenting a class-based exercise that leveraged VSD design charrettes, so that emerging designers and developers intentionally thought about the values they would embed in the design of future parental control apps. By using a VSD approach and working with college students, who are in a transitional period between late adolescence and early adulthood, we were able to progress toward balancing key tensions between parents and teens when it came to online safety, privacy, control, and autonomy. The end goal of this research is to convey the message that designs for adolescent online safety should be developmentally appropriate for teens.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: P.W.'s research on adolescent online safety is supported in part by the William T. Grant Foundation (#187941) and the National Science Foundation (IIP-1827700, IIS-1844881, CNS-1814439 and DUE-1643835). Any opinion, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the sponsors.

ORCID iDs

Karla Badillo-Urquiola https://orcid.org/0000-0002-1165-3619
Chhaya Chouhan https://orcid.org/0000-0002-2587-886X

References

Anderson, M., & Jiang, J. (2018, May 31). Teens, social media & technology 2018. *Pew Research Center*. Retrieved from http://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018/

Andrade, F. R. H., Mizoguchi, R., & Isotani, S. (2016). The bright and dark sides of gamification. In A. Micarelli, J. Stamper, & K. Panourgia (Eds.), *Intelligent tutoring systems* (pp. 176-186). Berlin, Germany: Springer International Publishing.

Arnett, J. J. (2000). Emerging adulthood: A theory of development from the late teens through the twenties. *American Psychologist*, *55*, 469-480. doi:10.1037/0003-066X.55.5.469

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). doi:10.5210/fm.v11i9.1394

Baumrind, D. (1987). A developmental perspective on adolescent risk taking in contemporary America. *New Directions for Child Development*, *37*, 93-125.

Blackwell, L., Gardiner, E., & Schoenebeck, S. (2016, February 27-March 2). *Managing expectations: Technology tensions among parents and teens*. Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW'16). Retrieved from https://yardi.people.si.umich.edu/pubs/Schoenebeck_ParentChildTensions16.pdf

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*, 77-101. doi:10.1191/1478088706qp063oa

Czeskis, A., Dermendjieva, I., Yapit, H., Borning, A., Friedman, B., Gill, B., & Kohno, T. (2010, July 14-16). *Parenting from the pocket: Value tensions and technical directions for secure and private parent-teen mobile safety*. Proceedings of the Sixth Symposium on Usable Privacy and Security, Redmond, WA. doi:10.1145/1837110.1837130

Davis, K., Dinhopl, A., & Hiniker, A. (2019, April 18). *"Everything's the phone": Understanding the phone's supercharged role in parent-teen relationships*. Retrieved from http://faculty.washington.edu/alexisr/everythingsThePhone.pdf

Davis, K., & Koepke, L. (2016). Risk and protective factors associated with cyberbullying: Are relationships or rules more protective? *Learning, Media and Technology*, *41*, 521-545. doi:10.1080/17439884.2014.994219

Dimock, M. (2019, January 17). Defining generations: Where Millennials end and Generation Z begins. *Pew Research Center*. Retrieved from https://www.pewresearch.org/fact-tank/2019/01/17/where-millennials-end-and-generation-z-begins/

Fails, J. A., Guha, M. L., & Druin, A. (2013). Methods and techniques for involving children in the design of new technology for children. *Human–Computer Interaction*, *6*, 85-166. doi:10.1561/1100000018

Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, *5*, 80-92. doi:10.1177/160940690600500107

Friedman, B. H., Kahn, P., & Borning, A. (2003). *Value sensitive design: Theory and methods*. Retrieved from https://faculty.washington.edu/pkahn/articles/vsd-theory-methods-tr.pdf

Friedman, B. H., Kahn, P. H., & Borning, A. (2006). Value sensitive design and information systems. In P. Zhang & D. Galletta (Eds.), *Human-computer interaction and management information systems: Foundations* (pp. 348-372). New York, NY: M.E. Sharpe.

Ghosh, A. K., Badillo-Urquiola, K., Guha, S., LaViola, J. J., Jr., & Wisniewski, P. J. (2018). *Safety vs. surveillance: What children have to say about mobile apps for parental control*. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems—CHI'18. Retrieved from http://www.eecs.ucf.edu/~jjl/pubs/pn1838-ghoshA.pdf

Havighurst, R. J. (1953). *Human development and education*. New York, NY: Longmans, Green.

Hiniker, A., Lee, B., Sobel, K., & Choe, E. K. (2017). Plan & play: Supporting intentional media use in early childhood. In *Proceedings of the 2017 Conference on Interaction Design and Children* (pp. 85-95). Retrieved from https://dl.acm.org/citation.cfm?doid=3078072.3079752

Hiniker, A., Schoenebeck, S. Y., & Kientz, J. A. (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 (pp. 1376-1389). New York, NY: Association for Computing Machinery.

James, C., Weinstein, E., & Mendoza, K. (2019). *Teaching digital citizens in today's world: Research and insights behind the common sense K–12 digital citizenship curriculum*. Retrieved from https://d1e2bohyu2u2w9.cloudfront.net/education/sites/default/files/tlr_component/common_sense_education_digital_citizenship_research_backgrounder.pdf

Jia, H., Wisniewski, P. J., Xu, H., Rosson, M. B., & Carroll, J. M. (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* (pp. 583-599). Retrieved from https://dl.acm.org/citation.cfm?id=2675287

Kerr, M., Stattin, H., & Trost, K. (1999). To know you is to trust you: Parents' trust is rooted in child disclosure of information. *Journal of Adolescence*, *22*, 737-752. doi:10.1006/jado.1999.0266

Khovanskaya, V., Dombrowski, L., Harmon, E., Korn, M., Light, A., Stewart, M., & Voida, A. (2018). Designing against the status quo. *Interactions*, *4*, 64-67.

Ko, M., Choi, S., Yang, S., Lee, J., & Lee, U. (2015). FamiLync: Facilitating participatory parental mediation of adolescents' smartphone use. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (pp. 867-878). New York, NY: Association for Computing Machinery.

May, J. (2001). Human–computer interaction. In N. J. Smelser & P. B. Baltes (Eds.), *International encyclopedia of the social & behavioral sciences* (pp. 7031-7035). Oxford, UK: Pergamon Press. doi:10.1016/B0-08-043076-7/01422-4

Mayseless, O., Wiseman, H., & Hai, I. (1998). Adolescents' relationships with father, mother, and same-gender friend. *Journal of Adolescent Research*, *13*, 101-123. doi:10.1177/0743554898131006

Mazmanian, M., & Lanette, S. (2017). "Okay, one more episode": An ethnography of parenting in the digital age. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (pp. 2273-2286). Retrieved from https://dl.acm.org/citation.cfm?id=2998218

McNally, B., Kumar, P., Hordatt, C., Mauriello, M. L., Naik, S., Norooz, L., . . . Druin, A. (2018). *Co-designing mobile online safety applications with children*. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. Retrieved from https://dl.acm.org/citation.cfm?id=3174097

Mitchell, K., Jones, L., Finkelhor, D., & Wolak, J. (2014). *Trends in unwanted online experiences and sexting* (Final report). Crimes Against Children Research Center. Retrieved from https://scholars.unh.edu/ccrc/49

Nouwen, M., Van Mechelen, M., & Zaman, B. (2015). A value sensitive design approach to parental software for young children. In *Proceedings of the 14th International Conference on Interaction Design and Children* (pp. 363-366). Retrieved from https://dl.acm.org/citation.cfm?id=2771917

Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation? *Journal of Family Theory & Review*, *2*, 175-196.

Pew Research Center. (2013). *Teens and technology*. Retrieved from https://www.pewinternet.org/2013/03/13/teens-and-technology-2013/

Rossler, B. (2005). *The value of privacy*. Oxford, UK: Polity Books.

Schilit, B., Adams, N., & Want, R. (1994). Context-aware computing applications. In *1994 First Workshop on Mobile Computing Systems and Applications* (pp. 85-90). Retrieved from https://ieeexplore.ieee.org/document/4624429

Spendlove, T. (2015). *Engineers use ROVs to save desert tortoises*. Retrieved from https://www.engineering.com/DesignSoftware/DesignSoftwareArticles/ArticleID/10783/Engineers-Use-ROVs-to-Save-Desert-Tortoises.aspx

Steinberg, L. (2004). Risk taking in adolescence: What changes, and why? *Annals of the New York Academy of Sciences*, *1021*, 51-58.

Williams, A. (2003). Adolescents' relationships with parents. *Journal of Language and Social Psychology*, *22*, 58-65. doi:10.1177/0261927X02250056

Wisniewski, P., Ghosh, A. K., Xu, H., Rosson, M. B., & Carroll, J. M. (2017). Parental control vs. teen self-regulation: Is there a middle ground for mobile online safety? In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (pp. 51-69). Retrieved from https://dl.acm.org/citation.cfm?id=2998352

Wisniewski, P., Jia, H., Wang, N., Zheng, S., Xu, H., Rosson, M. B., & Carroll, J. M. (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* (pp. 4029-4038). Retrieved from https://dl.acm.org/citation.cfm?id=2702240

Wisniewski, P., Xu, H., Rosson, M. B., Perkins, D. F., & Carroll, J. M. (2016). Dear diary: Teens reflect on their weekly online risk experiences. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 3919-3930). Retrieved from https://dl.acm.org/citation.cfm?id=2858317

Wolak, J., Mitchell, K., & Finkelhor, D. (2006). *Online victimization of youth: Five years later*. Crimes Against Children Research Center. Retrieved from https://scholars.unh.edu/ccrc/54

Youniss, J., & Smollar, J. (1985). *Adolescent relations with mothers, fathers, and friends*. Chicago: The University of Chicago Press.

Author Biographies

Karla Badillo-Urquiola is a third year PhD student at University of Central Florida. Her research interests lie at the intersection of human-computer interaction, psychology, and social computing. She studies adolescent online safety for teens in foster care.

Chhaya Chouhan is a first year PhD student in the Department of Computer Science at University of Central Florida. Her research focuses on mobile privacy and security. Her dissertation work aims to leverage community collaborations to help people make more informed and safe privacy decisions.

Stevie Chancellors is doctoral candidate in human centered computing at Georgia Institute of Technology. She builds human-centered algorithms to understand deviant behaviors in online communities.

Munmun De Choudhary is an assistant professor at Georgia Institute of Technology. Her research interests are in the interdisciplinary area of computational social science,

wherein she analyzes questions around making sense of human behavior and psychological state, as manifested via our online social footprints.

Pamela Wisniewski is an assistant professor at University of Central Florida. Her work lies at the intersection of social computing and privacy. She is particularly interested in the interplay between social media, privacy, and online safety for adolescents. She is an inaugural member of the ACM Future Computing Academy and the first computer scientist to ever be selected as a William T. Grant Scholar.