"They See You're a Girl if You Pick a Pink Robot with a Skirt": A Qualitative Study of How Children Conceptualize Data Processing and Digital Privacy Risks

Kaiwen Sun
kwsun@umich.edu
School of Information, University of Michigan
Ann Arbor, MI, USA

Carlo Sugatan
sugatanc@umich.edu
School of Information, University of Michigan
Ann Arbor, MI, USA

Tanisha Afnan
tafnan@umich.edu
School of Information, University of Michigan
Ann Arbor, MI, USA

Hayley Simon
hayleymi@umich.edu
Department of Psychology, University of Michigan
Ann Arbor, MI, USA

Susan A. Gelman
gelman@umich.edu
Department of Psychology, University of Michigan
Ann Arbor, MI, USA

Jenny Radesky
jradesky@umich.edu
Department of Pediatrics, University of Michigan Medical School
Ann Arbor, MI, USA

Florian Schaub
fschaub@umich.edu
School of Information, University of Michigan
Ann Arbor, MI, USA

ABSTRACT

As children become frequent digital technology users, concerns about their digital privacy are increasing. To better understand how young children conceptualize data processing and digital privacy risks, we interviewed 26 children, 4 to 10 years old, from families with higher educational attainment recruited in a college town. Our child participants construed apps' and services' data collection and storage practices in terms of their benefits, both to themselves and for user safety, and characterized both data tracking and privacy violations as interpersonal rather than considering automated processes or companies as privacy threats. We identify four factors shaping these mental models and privacy risk perceptions: (1) surface-level visual cues, (2) past digital interactions involving data collection, (3) age and cognitive development, and (4) privacy-related experiences in non-digital contexts. We discuss our findings' design, educational, and public policy implications toward better supporting children in identifying and reasoning about digital privacy risks.

CHI '21, May 8–13, 2021, Yokohama, Japan

ACM ISBN 978-1-4503-8096-6/21/05…$15.00
https://doi.org/10.1145/3411764.3445333

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; **Privacy protections**; • **Human-centered computing** → **Empirical studies in HCI**.

KEYWORDS

Digital Privacy, Children, Data Processing.

ACM Reference Format:
Kaiwen Sun, Carlo Sugatan, Tanisha Afnan, Hayley Simon, Susan A. Gelman, Jenny Radesky, and Florian Schaub. 2021. "They See You're a Girl if You Pick a Pink Robot with a Skirt": A Qualitative Study of How Children Conceptualize Data Processing and Digital Privacy Risks. In *CHI Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 34 pages. https://doi.org/10.1145/3411764.3445333

1 INTRODUCTION

Children increasingly use digital devices, such as smartphones and tablets (e.g., for watching videos, playing games) at an early age [54, 95, 96]. During children's online activities, they inevitably reveal information about themselves either actively or by passively leaving digital traces, which are collected by a multitude of applications and third parties [79, 85, 106, 128]. As a result, there have been growing concerns about children's interpersonal, institutional, and commercial privacy in the digital environment [75], such as online stranger danger [78], misuse or mishandling of sensitive family data by institutions [21], and monetizing children's data for profiling or behavioral targeting [85, 87, 128].

Laws such as the Children's Online Privacy Protection Act (COPPA) in the United States [34] and Europe's General Data Protection

Regulation (GDPR) [1] are meant to protect children's information privacy by restricting processing of children's data, requiring parental consent, and demanding age-appropriate privacy notices for children [36]. However, the effectiveness of these legal protections has been drawn into question [23], for instance, by many mobile apps skirting COPPA compliance [99]. Furthermore, while privacy notices have been suggested as a way to increase transparency about data collection, we still need a better understanding of children's awareness, understanding, concerns, and perceptions of the constantly evolving digital world and their conceptualization of the related privacy risks.

Previous work investigating children's privacy perceptions focused largely on older children and teenagers [31, 40, 58, 121, 125] or meta-cognitive approaches, such as asking children to define 'privacy' [90]. Few studies have focused on younger children's understanding of technology and associated privacy risks [75], and those that did focused primarily on specific aspects of children's online risk perceptions, such as children's ability to recognize different types of digital privacy and security threats, and parents' mediation strategies and the corresponding impact on children's digital risk perceptions [65, 84, 127]. We expand the investigation to a sample of younger children's understanding and conceptualization of digital privacy risks by focusing on their mental models of data processing (e.g., data sharing, collection, and inference), behavioral tracking and surveillance, and associated privacy risk perceptions through scenario-based semi-structured interviews with 26 children, aged 4 to 10 years old, from families with higher educational attainment recruited in a college town.

In brief, we found that our child participants (1) mostly construed apps' data collection and monitoring practices as being beneficial to them and ensuring safety of users; (2) characterized data monitoring and tracking processes as interpersonal (e.g., people watch them through the camera) instead of considering such processes as automated or performed by analytical tools; and (3) also conceptualized privacy violations primarily in terms of interpersonal interactions (e.g., involving bad actors or hackers) rather than considering companies as privacy threats. We identify four important factors that appear to shape children's mental models of data processing and perceptions of privacy risks: (1) presence or absence of surface-level visual cues related to data collection and processing, (2) children's prior experiences sharing information in their digital interactions, (3) children's age and cognitive development, and (4) children's privacy-related experiences in the non-digital world. We discuss our findings' implications for education, design, and public policy to better protect children's privacy in digital contexts.

2 RELATED WORK

Prior related work has investigated children's conceptualizations of privacy in digital and non-digital spaces, the role of both parents and the home environment in children's development of relevant mental models, and examined how children understand data flows and processing. We further discuss how interface design can impact children's understanding of technology.

2.1 Children's Mental Models of Privacy and Technology

By the age of four, children have rich conceptual structures embedded in broad explanatory theories, including in the social domain [52, 119]. This allows them to develop rudimentary understandings of more complex, layered concepts, including privacy, secrecy, and deception [129]. These initial concepts are typically rooted in their interpersonal experiences, and often tied to tangible objects or spaces. Most commonly, young children's descriptions of privacy include the ideas of being alone, being unobserved, and controlling access to physical places [48]. Bathrooms, for example, are frequently associated with children's conceptions of privacy as concrete 'private' spaces [48, 65, 90]. Absent from these definitions, however, is the concept of autonomy, or one's recognition of their own ability to manipulate or otherwise control their privacy. This can be recognized as a consequence of the limited agency children typically hold in other dimensions of their lives, and differs from adults and adolescents' definitions of privacy in which themes of autonomy are prevalent, and privacy concerns are seen as individual concerns dependent on individual actions [67].

As technological interfaces and internet-connected devices become more frequently adopted by younger children [54, 95, 96], young users are increasingly compelled to also develop perceptions of digital privacy [127]. Over 80 percent of children under the age of 11 use YouTube, many on a daily basis [14]. Tracking of preschool-aged children's mobile devices shows that they are avid users of streaming video services, apps, and mobile games [96]. Analyses of apps played by young children have shown a high prevalence of collection and sharing of persistent identifiers [99, 128], and in-app marketing approaches that may not be fully understood by young children [85]. Gelman et al. [37] found that child participants also expressed unfamiliarity with location tracking services on mobile devices, but showcased high levels of acceptance for this practice under specific conditions. Respective research has largely focused on understanding older children's, teenagers', and adolescents' privacy-related thought processes and behaviors [22, 123]. Younger children's mental models of technology and digital privacy have rarely been examined in depth [29, 75]. The few studies that exist suggest that children tend to simply translate their understanding of privacy in the physical world, and its governing rules, to that of digital privacy [65, 84, 127]. Children in the 7–12 age group, who are most represented across previous literature, were found to struggle with relating their norms of physical privacy to that of the digital domain. Most participants in a study done by Alias [8] expressed that it was more difficult to achieve privacy online than offline, as the internet was perceived to be overwhelmingly large and full of unknown people.

Related to these perceptions, the most commonly cited privacy concerns held by children within the 7–12 age group included talking and interacting with 'bad' strangers, coming across inappropriate content, or oversharing intimate information [127]. Still, the identification of these risks varied, and children's mental models of digital privacy was shown to display varying levels of inconsistency in how threats were perceived and responded to [84].

In our study, we investigate if relevant concerns resulting from the way children conceptualize data processing (e.g., data collection, data inference) and digital privacy risks emerge within even younger children in the 4–10 age range, and, more generally, what factors might shape children's mental models of data processing, behavioral tracking, and digital privacy risks.

2.2 Child Privacy and Parenting

In 2015, nearly 94% of U.S. children between the ages of 3 and 18 had access to a computer or smartphone at home, with roughly 61% of children having broadband access at home [64]. The responsibility of safeguarding a child's digital privacy at home is considered a parental duty [108]. Prior research has focused largely on parents talking with adolescents about social media privacy (i.e., what they post online) [107, 122] or use of website safeguards [76], but not how parents help children build understanding of data privacy. Most security-enhancing tools for children are predominantly marketed towards parents who are then charged with monitoring, restricting, or otherwise reviewing children's online activities [41, 81]. In a study conducted by Kumar et al. [65], children (nine years or younger) reported most likely seeking aid from a parent when confronted with something unknown online, and were also better able to navigate their digital privacy risks when following explicit rules laid out by their parents. Another study finds that children aged 7–11 reported trusting their parent or guardian to effectively protect them from technologies that the child identified as scary or threatening [124], while further work indicates that many younger children also rely on parental guidance for cues on data sharing [69].

Preteens and adolescents exhibit low levels of data literacy. Most participants in a study conducted by Bowler et al. [20] understood data abstractly as static, quantitative measures, and were unable to relate them back to their own personal contexts. Even prolific social media users in this age group were unable to describe how their personal data may be stored, shared, or manipulated by social media platforms [2]. While some connected the idea of "digital traces" to personal data, most did not then further connect those traces back to security, privacy, or personal harm [2]. Additionally, although children were able to offer conjectures about the ways data may flow, few exhibited awareness of the existing infrastructures within the data life-cycle [20]. When confronted with the realities of personal data tracking, however, teens exhibited negative or neutral reactions, with some reporting losses in empowerment as a result of the practice [30].

Parent attitudes and behaviors may shape child privacy perceptions. Parents who expressed particular concerns about their child's data, such as collection and selling of data by marketers, had higher adoption rates of some privacy protecting behaviors [33, 121]. Many other parents had as limited data literacy as their children, and while confused about what best practices to employ for protecting data, expressed being fearful of the potential consequences related to the mishandling or misuse of their personal data [21]. In fact, 63% of American adults report to understand very little about the laws and regulations that are in place to protect their privacy [15]. Parents who self-identified as less knowledgeable with regards to digital privacy were unsure regarding how to best protect their children online, and expressed low levels of confidence in their own guidance [107]. Children, whose parents effectively communicated potential online privacy concerns to them, had improved behavioral outcomes, with many of them more frequently engaging in privacy-protective behaviors (e.g., not sharing identifiable information online) [27]. This relationship changes when children become older. Adolescents identify parents as one of their greatest online privacy threats [24], especially when made aware of surveillance strategies deployed by their parents. Older children (8–11) also expressed discomfort with certain parental meditation strategies, such as the use of mobile phone monitoring tools [18], and showcased a dislike for other more general online behaviors that their parents engaged in (e.g., "sharenting," i.e., sharing children photos and information on social media [10, 111]).

Drawing from the multi-layered impacts that parental involvement could have on children's digital privacy perceptions and online self-protection behaviors, our study considers parents' digital literacy, online privacy perceptions, and mediation strategies toward their children's digital technology use to better contextualize and characterize our sample of child participants.

2.3 Understandings of Data Privacy and Interface Design

Finally, the gulf between individuals' privacy preferences and their data literacy has been shown to be partially related to misleading or obscuring user interface design choices across popular platforms, applications, and devices. This mismatch can usually be traced back to applications and systems behaving in ways that differ from users' expectations [68, 97]. These expectations typically stem from individuals' conceptualizations and mental models of system functionality, which are constrained by users' awareness of how certain digital phenomena operate, including invasive data collection practices [93].

Significant prior work has examined how poor accessibility and readability of privacy notices hinder the development of more accurate mental models [57, 86], but how surface-level interface design features of digital systems affect privacy understanding has been studied less. The way that interface design flaws may affect adults' privacy misconceptions has been previously examined with a specific focus on social networking sites [19, 118]. A lack of explicit visual cues was identified as a major design pitfall in these systems for supporting user privacy needs [118].

Regarding children, Hiniker et al. [53] studied how children in the 2 to 5 age range comprehend common UI elements. They find that digital interfaces littered with visuals that prove to be confusing for adult users, were even more perplexing for children who failed to grasp symbols readily understood by adults (e.g., progress bars) [53]. In our study, we investigate younger children's mental models of technology and identify interface surface cues as a key factor influencing their understanding of data processing, behavioral tracking, and privacy risk perceptions.

3 METHODS

To gain a deeper understanding of young children's mental models of data processing, behavioral tracking, and digital privacy risks perceptions, we conducted scenario-based, semi-structured interviews with 26 children in the 4–10 age range, complemented by

parental survey responses. Our study was conducted from August to December 2019 in the Conceptual Development Lab at the University of Michigan. Our study was approved by our Institutional Review Board.

3.1 Child Interview Protocol

After children and parents arrived in our lab, parents completed a consent form, including permission for their child to be audio and video recorded. Children were verbally informed about the study procedure and asked to provide verbal assent. Prior to the interview, the parent completed a brief form about their child's familiarity with certain devices and apps (see Appendix A).

One researcher then accompanied the child into the interview room, while the parent remained in the waiting area and completed the parental survey. If the child asked for the parent to be present, we invited the parent to sit with the child without engaging in the interview (two child participants did so, with age 4y6m and 6y7m). The interview was audio and video recorded through a one-way mirror. The interview (see Appendix B for the full interview protocol) began with warm-up questions asking the child about their device ownership and familiarity, usage habits, and preferences.

Next, we asked the child participant questions about up to three scenarios (video streaming, mobile gaming, and taking and messaging a photo) to elicit children's mental models of data flows and processing in different usage contexts. Gaming and video streaming are the most common digital activities among younger children [71, 127]. Many gaming apps collect children's data for behavioral tracking and targeted ads [85, 94], while also providing a space for children to interact with others online. Video streaming apps capture children's direct data input (e.g., content searches) and behavioral data traces to provide content recommendations. Videos also often include ads, which allowed us to investigate children's awareness of behavioral tracking, profiling, and inferences. We added the photo-sharing scenario because research has found that children share photos on social media [71, 127]. However, because younger children may not have much experience with social media, we instead asked children to take a photo and share it with the interviewer using a mobile messenger app, This enabled us to learn about children's understanding of respective data flows, including their awareness of intermediaries and platforms involved. For each scenario, we had a range of popular apps pre-installed on our study tablets (see list of apps in Appendix E),[1] with active subscriptions/accounts as needed. The tablet was stored in a box during the interview so that the child would not be distracted when they were not supposed to engage with the tablet. We only used the tablet as needed to help children explain how they used a particular app or point out specific app features and functions.

To aid us in choosing a first scenario, we asked the child about any popular apps they were familiar with, if necessary consulting the brief form completed by their parent. If the app mentioned was installed on our tablet, we proceeded with the associated scenario. If not, we asked about their familiarity with similar apps we had pre-installed. If the child had experience with more than one of the three scenarios, we asked the child to choose a scenario to start with. After completing the first scenario, the child had the option to move on to more scenarios or end the interview. Overall, 13 children talked about one scenario, 8 children completed two scenarios, and the remaining 5 children discussed all three scenarios. Each interview session lasted for about 30–60 minutes.

We designed five laminated cards indicating the different parts of the interview. These cards served as collectable tokens to help the child stay engaged and entertained during the interview (see Appendix F). One card for each of the three scenarios, and two cards representing the beginning and ending of the interview (airplane taking off; airplane landing). At the end, the child could exchange the collected cards for a toy.

For a given scenario, we asked about the child's experience with that activity, the corresponding app(s) they used. For a given app, we asked how the child thought the app functioned. We asked who the child thought created the app to understand whether they thought of individuals or companies, and what they thought a company was. We then asked whether an individual creator, or company, could see what the child did in the app to understand their perceptions of data traces, then asked more opened-ended questions on how and why an individual, or company, could do so. Next, we asked if and how apps could remember the child's activities online to understand their perceptions of data collection, storage, and transfer. Moreover, we asked the child if apps knew anything about them, such as their preferred content, to elicit the child's understanding of how data inferences worked in the app. We also covered questions regarding the child's interactions with different stakeholders (e.g., families, friends, strangers online) when using the app. We asked about their parents' rules about app usage, how the child decided on their username and identity online, and their understanding of advertisements in an app. If the child mentioned "bad people," "hackers," or related terms, we asked them to explain who those people were, and the risks the child associated with them. We ensured that the child had the opportunity to explain their answers. We concluded the interview by asking the child the types of information that apps knew about them, and how this could possibly happen.

3.2 Parental Survey

While their child was being interviewed, the parent completed a survey about their family characteristics (see Appendix C). We asked parents what digital devices they own, how much their child interacts with technologies, the child's usual daily media use duration, and types of digital activities the child engages in. We also asked about parents' usual mediation approaches (e.g., co-viewing, instructive, restrictive) using the Perceived Parental Media Mediation Scale (PPMMS) [114, 115], adapted to refer to mobile experiences (e.g., we changed "TV" to "apps"). We further asked whether and how they discuss digital literacy topics with their children, and what strategies they use to protect their child online. Next, we measured the parent's internet skill level and information privacy perceptions using the Internet Skills Scale (ISS) [117] and the Internet Users' Information Privacy Concerns (IUIPC) [80]. Lastly, we asked for the parent's demographic information.

[1] Based on a child's familiarity with iOS or Android, we used either an iPad or an Android tablet during a study session. The same apps were pre-installed on both devices.

3.3 Recruitment

We recruited participants from our existing child development lab database, which includes contact information for a large number of families who have previously expressed interest in participating in research studies with children through in-person sign-up opportunities (e.g., community events), direct mailings, and email lists. We also used snowball sampling to recruit further participants to increase sample diversity. Each participating family received $25 in cash and a toy the child could choose.

3.4 Data Analysis

The 26 interviews were video recorded. We manually anonymized audio files, which were then transcribed using a transcription service. A team member reviewed and corrected the transcripts' consistency against the videos, as well as added notes on non-verbal behavior (e.g., child nodding or shaking head).

We completed data analysis in two phases. During the first phase, we randomly selected seven interviews and used affinity diagramming to group quotes that revealed similar themes [55]. After we completed all 26 interviews, the first author went through all transcripts and created analytic memos to identify emergent themes and categories [102]. In the second phase, the first author integrated the emergent themes from affinity diagramming and the analytic memos to develop the initial codebook, which was further refined based on team discussion and feedback. Using the updated codebook, the first two authors coded several interviews while iteratively refining the codebook by clarifying code definitions and resolving disagreements. The first two authors completed all the coding in three phases, with each phase focused on one specific part of the codebook (we divided the codebook into three parts: conceptualizations of data processing, reliance of surface cues, and risk perceptions and self-protective behaviors) until reasonable inter-rater reliability was achieved (Cohen's κ = .79, .80, .75, respectively). Then the first author (re-)coded the first two parts and the second author (re-)coded the third part for all transcriptions.

The final codebook consisted of 70 codes in 33 categories (see Appendix D), including a combination of descriptive codes (e.g., risks from exposing one's information), structural codes (e.g., other people's view of one's account/activities), process codes (e.g., self-protective behaviors), concept codes (e.g., definition of 'personal account'), value codes (e.g., attitude toward app's memory/knowledge of user and user's behaviors), and causation codes (e.g., ways that app can or cannot monitor/track/watch people) [102].

We limited parental survey analysis to descriptive statistics in accordance with the qualitative nature and sample size of our study. Given that we adjusted wording of some PPMMS items [114, 115], we validated internal consistency of its sub-scales (co-view subscale: Cronbach's α = .78; instructive sub-scale: Cronbach's α = .85; restrictive sub-scale: Cronbach's α = .89).

4 DEMOGRAPHICS AND MEDIA USE

Demographics and Media Use. For the 26 participating families (see Table 1), there were 12 boys and 14 girls (age range: 4y6m to 10y8m, median age: 8y7m), all of whom attended school. Parents self-identified as White (18), African-American (1), Asian (3), Latinx (2), and Other (2). Almost all parents were highly educated with bachelor or postgraduate degrees and employed in diverse occupations.

All children regularly used smartphones and tablets. More than half (15) started to interact with Internet-connected devices around or before the age of two. Almost all families had multiple digital devices to access the internet (e.g., computer, smartphone, tablet). Ten children had their own tablets. All children used media throughout the week or over the weekend, ranging from 30 minutes to a few hours daily. Most engaged in content consumption activities (e.g., playing games, watching videos), about half used communications apps (calls, texting, video chatting), half listened to music or audiobooks, and a few children read electronic books.

Parental Mediation Strategies. According to their PPMMS responses, parents in our sample reported using all three mediation approaches (co-view, instructive, and restrictive) "sometimes" with their children. The restrictive approach was used slightly more often (mean=3.15, SD=.72) than the other two (co-viewing: mean=2.71, SD=.7; instructive: mean=2.62, SD=.73), which indicates that these parents were likely to set rules on children's app and media use. Half of the parents with school-aged children reported talking with them about video and game content (e.g., what characters were doing, violence) at least sometimes or more frequently. Six parents with older children (3rd–5th grade) sometimes talked about app permissions and the types of collected data. Ten parents of school-aged children pointed out design features that encourage continued app use (e.g., autoplay, daily rewards, notifications) to their children sometimes or more often.

Parental Internet Skills and Online Privacy Perceptions. According to their ISS responses, all parents exhibited high competency with mobile devices (mean=4.51, SD=.44), social technologies (mean=4.53, SD=.49), operating digital devices and media (mean=4.58, SD=.41), and information navigation (mean = 4.02, SD=.64). Parents further scored highly on the IUIPC subscales, indicating that they were generally concerned about personal information collection by companies (mean=4.33, SD=.60), wanted control over their personal information (mean=4.15, SD=.66), and were aware of companies' privacy practices (mean=4.49, SD=.45).

5 FINDINGS

We discuss two aspects of children's mental models of data processing and digital privacy. First, how children conceptualize data sharing, collection, and inference; and second, how they understand behavioral tracking and surveillance. We then present children's digital privacy risk perceptions, and their self-protective strategies in response to those perceptions.

5.1 Children's Mental Models of Data Processing

We found that children in our study tended to (1) conceptualize mobile app data as being static and local to their device, (2) use teleological reasoning to make sense of why apps collect their data, (3) believe that inferences about them can only be made based on their in-app behavioral data, and (4) understand that their prior app use and activities can reveal their preferences, which apps can use to make content recommendations.

Child	Age	Gender	Grade	Interview Scenario(s)	Parent Education	Parent Occupation	Parent Ethnicity
CP1	4y6m	M	Preschool	Video	Advanced degree	Staff in Education	White
CP14	5y3m	F	Kindergarden	Photo	Advanced degree	Nurse Anesthetist	Latinx
CP26	5y6m	M	Kindergarden	Game	Bachelor's Degree	Clinical Specialist	White
CP13	5y7m	F	Kindergarden	Photo, Game	Advanced degree	Manager, Non-Profit	Asian
CP16	6y1m	M	Kindergarden	Game	Advanced degree	Homemaker	White
CP19	6y2m	F	1st grade	Game	Advanced degree	Clinical Social Worker	White
CP24	6y3m	F	Kindergarden	Game, Video	Advanced degree	Administrator	White
CP22	6y6m	M	1st Grade	Video	Bachelor's degree	Business Coach	White
CP18	6y7m	M	1st Grade	Photo	Advanced degree	Teacher	White
CP25	6y9m	M	1st Grade	Game	Bachelor's Degree	Nurse	Asian
CP21	6y11m	M	1st Grade	Video	Advanced degree	Consultant and Coach	White
CP7	7y2m	M	2nd Grade	Game, Video	Bachelor's degree	Homemaker	White
CP3	7y6m	F	2nd Grade	Photo, Game, Video	Bachelor's degree	Homemaker	White
CP10	8y6m	M	3rd Grade	Game, Video, Photo	Trade/Vocational	School Official	Black
CP27	8y8m	F	3rd Grade	Video, Game	Advanced degree	Executive Director	White
CP8	8y9m	M	3rd Grade	Game, Video	Bachelor's degree	Education	White
CP2	9y0m	M	4th Grade	Game, Photo, Video	Advanced degree	Librarian	White
CP12	9y0m	F	4th Grade	Video	Bachelor's degree	Teacher	Other
CP9	9y10m	M	4th Grade	Game, Photo	Advanced degree	Interior Designer	White
CP4	10y0m	F	5th Grade	Photo, Game	Advanced degree	Physician	White
CP20	10y1m	F	4th Grade	Game, Video	Bachelor's degree	Software Architect	White
CP15	10y3m	F	5th Grade	Video, Game, Photo	Bachelor's degree	Registered Nurse	Other
CP17	10y4m	F	5th Grade	Game	Advanced degree	Project Assistant	White
CP23	10y6m	F	5th Grade	Video	Advanced degree	Teacher	White
CP11	10y8m	M	5th Grade	Game, Video, Photo	Advanced degree	Counselor	Latinx
CP5	10y8m	F	5th Grade	Video	Advanced degree	N/A	Latinx

Table 1: Child and Parent Demographics. Interview scenarios are listed in order of completion.

5.1.1 Data is static and stored locally. Bowler et al. [20] found that some teens believe that data "lives" in a fixed place and tends to be static. Overall, our child participants shared a similar notion. They believed that data was stored on the device or stored inside an app locally, rather than understanding that data is often saved in companies' backend systems. Most children expressed understanding that apps and platforms "remembered" things about them, and some appeared to draw conclusions from the apps' user interfaces that showed their progress in the game or what videos they liked. These children also believed that they had control over "what apps remembered about them." For example, some children stated that they could delete or close the app to stop the app from remembering their data, but were not aware of how data might be transmitted to other places that children would not have direct control over.

Over half of the children mentioned data storage locations, ranging from on the local device to "in the app," but none indicated that data constantly flows between the device/apps and backend servers. Only a few older children mentioned the "cloud," but did not articulate what it is or how it worked. Other children referred to local device storage or specific places in the app. For instance, CP15 (10y3m) explained how apps could collect and save her data locally, *"because there's probably like a memory that they have that people who made it would have a memory, not memory like physically but memory on the computer or a laptop of what you did."* Similarly, CP02 (9y0m) said *"I think that the iPad just stores it [photos in the photo app] in its memory."* Those children who thought that their data was stored in a specific place in the app tended to vividly refer to the app's user interface. CP08 explained where a game stored her progress data, *"There's always a button or if you finished a Candy Crush level, it'll show you a pathway that leads farther and farther. I think that's where they keep your progress in Candy Crush."* CP23 (10y6m) disclosed where the app kept the data about her:

> *"Usually if you are typing in something and you have used YouTube before, usually has a little box underneath what you are searching [...] And then underneath that there will be a little bar called, it says search history and then it shows some of the videos you have watched."*

Children frequently referenced similar app surface cues such as "the search box," "continue to play for [child name]," or a game's "save and quit button," as storage places of their progress data. However, if the respective visual cues were absent, children assumed that no relevant data was remembered, not mentioning about 'hidden' data storage or collection methods. An older child, CP15 (10y3m) pointed out only certain types of data that were visible to her would be collected by the game app: *"well, they [game apps] might remember my progress, but it's not like, 'She did this slick [game feature] at like 0.24 seconds.' I mean, they sometimes remember my record. Like in Slither IO [game name], it's how big you get, but not anything suspicious."*

Considering that children seemed to have learned through the apps' surface cues about how their data was collected, most children

(6y7m–10y8m) described how they could influence what the app "knew" about them (i.e., data collection from the app) by exiting or removing the app visually. A few younger children (6y7m–7y2m) talked about turning the device off or exiting the app foreground, so it is not visible anymore, can stop the app from collecting data. Some older children (9y0m–10y3m) said that deleting the collected data in the app or removing the app entirely would stop the app from collecting information. In other words, by removing surface cues, children believed they could remove the collected data, even though in actuality, apps may still be running in the background or have data stored on their servers.

Only one older child, CP04 (10y0m), was aware that the data people shared on social media would be out of their control as deleting the app would not affect the collected data, and explained such understanding in the context of Facebook, *"like Facebook you can sign in and then it always remembers you even if you deleted it."*

5.1.2 Data collection is for convenience and benefit. Data can be categorized into three types: data given or published, data traces, and inferred data [116]. Our child participants' understanding of data centered around the "data given" category. They were generally aware that they hand over data to an app when entering personal information (e.g., for account registration). Most of the children in our study across all ages understood, to some extent, that their personal and behavioral data was collected so apps could remember what they did, such as their current game level, how many coins they had collected, or what videos they had watched. These children described this as convenient like CP11 (10y8m) explained: *"I think they [apps] can remember [your progress] because they want you to feel the experience of not restarting over...I think it's nice that it saves it [my progress] so I can just press the go back to what I was listening to button."*

We interpret this as a teleological mode of explanation, that is, explaining events and structures as existing for one's purpose or benefit, which is an intuitive mode of explanation for young children [60–62]. Half the children viewed the purpose of app storage as benefiting the user, to give them easy access to where they last stopped in a game or video, or providing a record of their digital progress. A few older children mentioned that collected data could be used to improve user experience. CP11 (10y8m) said, *"I think maybe it [YouTube] stores the progress of all of the videos [people watch] and it makes sure that you have a good experience, maybe."* Five older children (8y6m–10y8m) realized that companies also derived benefits from collecting people's data, but still focused on how it can improve the app functionality and content for the user. CP08 (8y9m) said, *"because then they [apps] get to see, they can make more tweaks to the game. They can see progress that you're making."*

Only two older children expressed concerns over data collection. CP04 (10y0m) vaguely talked about potential harms apps could do with the collected data (*"they can do bad things"*), while CP09 (9y10m) described businesses exploiting users and their data for financial gain: *"It [the app] remembers what you like more, and gets you more addicted to make it happen more ... so they can make more money. But the less people who play, then the less money they make."*

5.1.3 Inferences linked to in-app behaviors. From our data, we identified children's understanding of data inferences as a subset of "what the app/company knows about you" (a question we asked in our interview). These inferences were primarily based on two types of information: 1) children's digital activities they were aware of, such as the type of show they remembered watching in a video app; and 2) data that children inputted directly, as when typing their name when creating an app account. We found that most children understood these simple data inferences and attributed them to their own in-app activities. Only two children indicated a more in-depth understanding of data inferences that were profiled through aggregation and analysis of people's shared data, data traces, or other data sources [116].

More than half of the children (6y1m–10y8m) recognized that their in-app behaviors allowed the app to infer what they like, *"because YouTube could sense what game you pick on. So he probably knows what games you like or what you click a lot,"* (CP21, 6y11m); their skill level, *"some reading games, they might if you were doing a really hard book, they would see that you're a really good reader. If it was a really easy book, they might see or they could tell what grade you're in depending on how well you read" (CP08, 8y9m)*; and their personal characteristics such as gender, age, personalities, and personal styles. For instance, CP02 (9y0m) explained: *"[the app can estimate age] because of how, what shows we watch, but not like the exact age...Yeah, [the app knows that] he's [the child himself] not a teenager...'Cause he's like, six to ten [based on the types of shows he watched]."*

Similarly, CP05 (10y8m) explained, *"if you like to customize things [in the app], then it'll probably know your style."* And CP12 (9y0m) reported that *"the things you do on it [the app] will tell them [the app creators] like what you like to do and like what's your personality."*

When talking about the possibility of inferring gender, several children (6y2m–9y0m) expected that apps would make gender-stereotypical inferences based on their in-app activities. CP12 (9y0m) said that Netflix would know children's gender because *"If you're a boy you probably want to watch boy shows like Minecraft or like Spiderman or something. Or if you're a girl, you're probably more likely to watch My Little Pony or Barbie (laugh)."* Similarly, CP08 (8y9m) said:

> *"We get to choose ... what our robot [game avatar] looks like. I think they [apps] could see if you're a boy or girl. If you did a pink robot with a skirt [the app would know you're a girl]...[but] if you're a girl, you liked blue and you liked Star Wars or something, and you put instead of pink and purple you put blue and red [the apps would not know your real gender]."*

Additionally, several children (all older than 7) indicated that the apps could not conclude more information about them because they had never put in any personal information. CP27 (8y8m) explained that the game Crossy Road would not know anything about him, *"because I did not put anything in there that talks about me."* Also, a few children did not believe that apps could find out their location without directly asking. CP15 (10y3m) indicated this as a safety issue, *"I think they [apps] cannot ask for that [your location]. Nobody would sign up for a website if they asked where you lived."*

Only two older children suggested that an app might make inferences that were not based on their own in-app behaviors but rather more sophisticated information usage. One child (CP12, 9y0m) indicated an understanding of location tracking based on the device,

"Because where the iPad or like thing [device] is that you're using for it. They'll [the apps] probably know where that [device] is. So they'll probably know where you live too." Another child (CP20, 10y1m) showed an appreciation of inferences based on a comparison of data across users on the YouTube Kids platform:

> *"[YouTube Kids] would see that you [are] usually watching this and this. So then they would put more things like that and see if you would do them and then they would kind of figure out how, what you like and [...] try and figure out your age or gender by what other people that have the same age or gender are liking. But that probably isn't usually that accurate."*

It is likely that CP20's sophisticated understanding of data inference is related to active parental involvement as her parent worked in the tech industry and, in the parental survey, reported often explaining to her aspects of the data collection and online safety.

5.1.4 Content recommendations are based on prior digital activities. When children were describing whether apps knew what videos/games they liked to watch or play, or why they might see different app content than others, they accurately believed that their prior interactions and activities in the app revealed their content preferences, and that apps would use such data to make content recommendations.

Most of the 7–10-year-olds in our study recognized that apps tailored content recommendations to either be similar to what they had interacted with before or, to some extent, matched their preferences. Some children explained that such recommendations depended on their prior activities in the apps such as *"what games you play"* (CP02, 9y0m), *"what you watch, and who you subscribe to"* (CP10, 8y6m), *"if you dislike it on them...or if you like it"* (CP11,10y8m), or *"if I watch something or I search it a lot"* (CP20, 10y1m). Some of them explained how apps' visual cues shaped their understanding of how recommendations worked. For instance, CP03 (7y6m) mentioned Netflix' recommendation categories:

> *"So, if I've been watching, uh, StoryBots, and other shows that the StoryBot company does, and other shows like StoryBots. I think that's how it tells what stuff I watch and I like to watch... It'll be like, one of those isles [Netflix interface of horizontal scrolling] 'Because you watched StoryBot' so, it gives you some other shows you might like."*

An older child, CP05 (10y8m), reasoned how YouTube's content recommendations work, and how she could influence them with her behaviors,

> *"I think it [YouTube] matches what you watch a lot, and then tries to lead you towards other videos that they think would be interesting to you. Like if you like... gaming videos...you just watch it a lot, and then it just thinks that maybe you just like to watch this stuff, and give you more and more of it...Sometimes they show the same videos a couple of times, because they think that you'll like it. But then if you don't press on it for a while, then it'll go away... It probably will [know what you like or don't like], because if you like to customize things, then it'll probably know your style."*

CP12 (9y0m) explained in similar terms how Netflix would know her content preferences: *"Every time you watch something they record it so they know what you like to watch. If I like watching things that are like, really violent or something maybe they'll know, because I always watch stuff like that."*

A few children explained how this content personalization results in different people getting different content recommendations. CP10 (8y6m) noted that *"different people watch different things, so that something different will pop up on [their] recommended page."* Similarly, CP11 (10y9m) said *"I think it [YouTube] shows different [videos to different people], of course, because everybody has a different preference."*

Expanding from content recommendations within the app, CP15 also talked about how app recommendations in the app store are based on her previous downloads, and that a new device would not be able to make suggestions for users unless they download apps first :

> *On the App Store...I have downloaded the app with my parents' permission before. It says like suggestions for you and you can scroll through there and see if you like it, but if you go like say this is a brand new iPad and you're new to it, then you could...if you start downloading things on it, it might start popping up suggestions for you, like one or two things.*

5.2 Children's Mental Models of Behavior Tracking and Surveillance

We identified children's mental models of behavioral tracking and surveillance centered on (1) data tracking and monitoring occurring only on an interpersonal level (i.e., another person watching them), not considering large-scale, automated data analytics and (2) believing that monitoring is to be used for app functioning and safety, not considering any secondary uses, privacy risks, or harms. In contrast to content recommendations, (3) children were unaware that ads they encountered are targeted to them based on information collected about them.

5.2.1 Monitoring is interpersonal. Children in our study described behavior tracking and surveillance processes in an interpersonal way that always involved some form of human engagement (e.g., observation) in a one-to-one relationship. First, it should be noted that children rarely mentioned privacy issues spontaneously, and only discussed privacy in response to probes by the interviewer; it often appeared that they had not considered that companies or platforms would want to monitor their behavior for reasons other than the convenience-related purposes mentioned before in Section 5.1.2.

When asked about data tracking and monitoring, some 5–10-year-olds provided explanations involving a one-to-one mode and interpersonal monitoring metaphors, such as being visually "observed" by cameras, people logging into their accounts, people viewing their screens, or people having to be physically present to observe them rather than being able to do so through data collection about their behaviors. For instance, some children used the absence or presence of cameras to explain how monitoring works. CP07 (7y2m) believed that monitoring would require cameras in

the game, *"if he [Minecraft creator] was watching us there would be cameras in Minecraft."* CP19 (6y2m), instead suspected that an app could see him through the computer camera, if he did not cover it. CP12 (9y0m) shared a similar belief but specifically thought the people behind an app would watch him through a camera to see what he likes, *"Since they [Netflix creators] make the Netflix company, they like watch over the cameras on their screen maybe to like see what you like to watch."*

This association of tracking from individual employees at app companies was expressed by a few children. They assumed these people would receive direct data such as children's preferred content or in-app activities. CP19 (6y2m) stated that *"the person who made the game, whenever someone starts playing that, I feel like they get an email saying, 'someone is playing My Tom 2,' or 'Someone is playing YouTube.' "*.

Two older children, CP11 (10y8m) and CP23 (10y6m), thought monitoring was a human action that was impossible to be achieved in the app because *"if they did [monitor you], then they would have probably thousands of people to look at ... I don't think that they could do that, possibly,"* and *"there are so many people using YouTube all the time [so the YouTube creator cannot monitor so many people]."* Additionally, a few younger children said either the app creator is *"somewhere else,"* or *"the app cannot see you [so it cannot monitor you],"* indicating that an absence of people or interpersonal actions meant data monitoring could not occur.

While our child participants predominantly conceptualized monitoring as interpersonal, two children demonstrated an understanding that monitoring was achieved through data collection of their digital behaviors. CP04 (10y0m) said:

> *"they [game app creators] can probably see [what I did in the game app] because you have to go into the game... they know that someone downloaded that game, so they know that you downloaded the game...And they know that they can watch you and the moves you do."*

CP21 (6y11m) indicated a similar idea *"they [the apps] remember you like tapping a lot. Like 'hey that guy looked that up.' "* Nonetheless, these examples still referred to individual human actors looking at the data, and did not go so far as to ascribe a commercial purpose to monitoring user behavior.

5.2.2 Data monitoring purposes differ from data remembering. As we described in 5.1.2, children considered that apps remember what they did to make it easier for them to resume or improve the app. We found a nuanced difference in how children reasoned about the purpose of data monitoring and tracking when asked whether apps could see what they were doing in the apps.[2] Some children concluded that monitoring occurs in order to benefit the app itself such as controlling users' proper use of the apps, maintaining a safe environment, and improving the app experience. For instance, two children both mentioned that apps needed to watch people to ensure proper use of the app: *"They (app companies) can see what people are doing so that they make sure people aren't using their stuff the wrong way or something, like copyrighting"* (CP12, 9y0m). Similarly, CP19 (6y2m) said, *"I think that they're (people who made the app) watching to make sure that we don't make anything on it to make like a virus."*

Two older children explained that app creators or companies need to stay in control for safety purposes, such as watching out for hackers and detecting suspicious behavior. CP15 (10y3m) mentioned, *"They (app creators) also need to stay in control of YouTube and make sure that somebody doesn't try to take over YouTube or hack into the system"*. CP05 (10y8m) said,

> *"I think that they'll need to get your permission [the YouTube creators to see your YouTube activity], or if they think you're doing something suspicious, and trying to hack it or something... maybe they can like see everyone's accounts or something, and then they'll get notices if there's any odd behavior ... to make sure that their app is safe."*

Notably, CP05 assumed that, by default, YouTube would ask users for permission before monitoring their behaviors, and felt that direct monitoring was only reasonable if YouTube detects suspicious activity.

More in line with assumed purposes for data collection and storage as we described in Section 5.1.2, two children explained how (game) apps would monitor users to improve the playing experience, *"Because they've designed the game so they might be able to see what, how it's working so that they can make it better and change"* (CP20, 10y1m); and *"Sometimes there's challenges and I think they [app company] create the challenges to see how well you are [in the game]... to see if they can add any more little tips or something to make it a little easier or more fun"* (CP08, 8y9m).

5.2.3 Ads are annoying, but not targeted. Most children in our study talked about ads as a salient element of their digital experiences, but most did not seem to understand that ads were targeted to them based on their tracked online activities. However, a few older children drew the connection between their online activities and ads they received.

Most children (5y6m–10y8m) mentioned seeing ads when using apps, largely in-game or YouTube ads. These children usually perceived ads as a disruption of their digital activities they had to get past: *"press the x button"* (CP08, 8y9m), *"pressed skip"* (CP11, 10y8m), or *"put it [device] down and wait for it [ads] to go away"* (CP05, 10y8m). CP17 (10y4m) complained about annoying in-game ads with persuasive intent:

> *"Like Toon Blast [a puzzle game], for example. That [ad] pops up every time, and it's like, 'Toon Blast!' And it gives me this example with this girl. Well, it's her finger, and she's just pressing them, and then at the end, it's like, 'Toon Blast!' And it's like, 'Click here to buy!' Or like, 'Click here to get it!' But sometimes it makes you play it, which is kind of annoying. And it's like you can skip in 26 seconds or something like that."*

Three children mentioned they had learned about or tried new games because of ads, so they considered ads to be helpful sometimes. Most children (5y6m–10y8m) reasoned that ads were placed by the app companies or content creators for various purposes such as recommending new products and making money. Most children did not realize that ads were customized to them and had different

[2]We asked about 'seeing' as it is a concept easily understood even by young children, and to avoid priming or confusing them with tracking or monitoring.

ideas on how ads worked for different people. For example, some thought everyone received the same ads, *"because YouTube Kids can show a bunch of different ads at more than one time"* (CP07, 7y2m). Some thought that people could get the same ads but definitely *"not at the exact same time"* (CP08, 8y9m), and CP17 (10y4m) further explained, *"if one ad's happening, then maybe it cannot happen somewhere else."* Other children thought certain ads would be shown for the same video at the same time, similar to TV ads, *"Because if people are watching the same video at the same time, then I'm pretty sure the ads will come at the same time and they will show the stuff at the same time"* (CP19, 6y2m).

Several older children (8y6m–10y8m) understood that ads are customized based on one's preferences, in-app activities, and locations. CP10 (8y6m) explained, *"It's [the ads that you get] based on what you watch and what you like to watch, and there are different ads so it's easy for the YouTuber to just put down an ad, and different ads will show up on different people's screens."*

Also note how CP10 described the ad selection to the content creator (the "YouTuber") rather than the platform (YouTube). CP23 (10y6m) noted correctly that location affected what ads people get, *"If you are here you will not get the same results as a person in Japan. They will not get the same ads because... There are a lot of companies that are particular to like one country."*

5.3 Children's Privacy Risk Perceptions and Behaviors

Children's mental models appeared to impact their online risk perceptions and self-protective behaviors as they tended to be concerned about exposing personal information online, being identified by bad online actors and the resulting harms, and having their data collected and used by companies for nefarious purposes. Children in our study mostly conceptualized digital privacy in an interpersonal manner that requires active provision of personal information. Thus, their privacy behaviors center around (1) trusting and interacting with families and friends online while avoiding disclosing personal information to strangers; (2) having positive attitudes toward data being used for their convenience and user benefit, but negative attitudes toward data collection of information they were unaware of sharing, data misuses, and data breaches; and (3) perceiving risks as primarily physical in nature (i.e., online strangers hurting them). They described corresponding self-protective behaviors in reaction to such risks.

5.3.1 Online privacy risk perceived as interpersonal. Third et al. [113] found that children mainly focus on interpersonal aspects of privacy online as they worry about their private digital world being monitored by parents, and breaches of private data by friends or hackers. In comparison, children in our study almost always talked about their digital activities with parents, and parents' guidance influenced children's decisions on what content to consume online. Most of the children interacted with or shared their online activities with friends. Online strangers and bad actors were two out-group stakeholders children considered risky to interact with, so children were cautious not to share personal information with these people.

Parents were considered as the inner circle guardians to children's digital space by many of our participants. Some children who were older than 7 years shared with parents openly what happens in their digital space, ranging from having parents as the exclusive contact in an app, relying on parents for digital purchases, to using parent's credentials for app logins. Some children (6y1m–10y8m) relied on their parents for evaluation of what content is appropriate (*"I want to check in with them to make sure that it's [the game] safe,"* CP15, 10y3m) and supervision (*"I usually have to tell them or I have to watch in the room they are in,"* CP07, 7y2m).

Friends were a second commonly mentioned in-group stakeholder. Most children (5y3m–10y8m) in our study generally interacted with friends online or discussed their online experiences with them. However, they had mixed feelings about the level of detail to tell friends about their online activities. Some children were happy to share almost everything with their friends so *"they might decide to go onto the same game and play with me"* (CP05, 10y8m). Some thought their online behaviors were private information they would have to explicitly share with friends (i.e., *"I don't have to share everything about me,"* CP11, 10y8m), or worried about friends' disapproval like CP21 (6y11m) said: *"I might do a game that they don't like and they laugh at me. Yeah, that had happened to me. Cause [friend name], I was playing Minecraft when [friend] was like, 'What was that?' Minecraft. 'I do not like Minecraft, ha ha ha.' "*

Other children chose what to tell and which friend to tell based on whether *"some friends are nice to me"* (CP13, 5y7m) or *"whether they're good friends and they would not make fun for what I watch or they would not criticize what I watch, then I feel fine with it."* (CP15, 10y3pm). CP15 continued, *"But if there's somebody that knew that I watched a certain video and then they watch they see that this was really bad and then told me the next day that your interest are really, really weird then I would feel bad about it."*

Almost half of the child participants (6y2m–10y8m) mentioned other online users, such as strangers, and most of them believed that these strangers may have bad intentions. As a result, children mentioned avoiding interactions and revealing personal information to other online users. CP19 said she would not play games with strangers online because *"they might hack into our account and mess it up and make it have a virus to make it kicked out, like whenever we join the game it just kicks us out."* CP25 (6y9m) mentioned possible physical harm from interacting with strangers online, *"if it's an adult, they might be trying to kidnap you secretly."* A few children were more open towards strangers, noting that strangers can be normal users or good people too. CP10 (8y6m) said he would play games with other people online because if *"they're good people, they won't hurt you."* CP1 (10y3m) cared about the comments from other users, *"if they criticize you about it [what videos you watched] then I feel bad, if they let's say like share the interest with you, then I feel fine about it."*

5.3.2 Older children perceived risks of data collection. While most of our child participants, especially those under the age of 7, held positive attitudes towards data collection because of perceived benefits, some older children, all older than 8 years, reasoned about risks stemming from data collection. For instance, a few children expressed privacy concerns depending on what data apps collected and how they used it. CP11 (10y8m) worried about data breaches, *"sometimes I think it's bad [that apps collected your data] because maybe if you do get hacked or you accidentally do something bad on it."* CP15 (10y3m) commented that the app might use collected data

for nefarious purposes, like *"keeping stuff that is sort of private and it could be keeping that and finding out information about you."*

Other children disliked that apps collect "private information" about them or directly monitoring them. CP27 (8y8m) noted, *"It's good if they remember your high score [in the game], but not if you put stuff about you in there [and the app remembered]."* CP17 (10y4m) liked when games keep track of which level she was on *"but if they watched me when I was playing, then I don't like that."* Both reasoned about the types of data collection or purposes they would be comfortable with, distinguishing between those that provide convenience and others that might affect their privacy.

5.3.3 Digital privacy risks primarily lead to physical harms. Some children in our study mentioned "bad people" as threats to their online safety and privacy, including cyberbullies, robbers, bad people working for the app company, and strangers. These children (older than 6 years) believed that bad people would *"steal my password ... delete my Minecraft account ... make friends with other people that I don't want to be friends with ... or send money."* (CP11, 10y8m), *"hack into your system"* (CP08, 8y9m), *"cyberbully somebody"* (CP15, 10y3m), *"delete other people's videos"* (CP05, 10y8m), *"steal your information"* (CP10, 8y6m), and *"find things about you"* (CP20, 10y1m).

More than half of the children (5y7m–10y8m) discussed potential harms of exposing their personal information (e.g., username, password, address) online. Particularly, several younger children (5y7m–7y2m) related online privacy risks mostly to physical harm, *"they [online strangers] might steal me"* (CP14, 5y7m), and *"if you give them your address they'll look for it, and then if they have a knife or gun or sword they will try to kill you"*(CP07, 7y2m).

While younger children generally did not see risks in using their real names online, nearly half of the children (7y2m–10y6m) recognized both physical and digital risks of using their full or partial real name as usernames, such as *"steal my identity"* (CP17, 10y4m), *"see your real name and like try to use it to get into like some of your other accounts"* (CP12, 9y0m), or *"look you up and figure out where you live, and beat me or be mean"* (CP04, 10y0m). CP23 (10y6m) further noted that not using one's real name, means that if their account gets compromised *"it does not give any information about you."* This suggests a substantial age-based difference in children's understanding of risks of sharing their real identity online.

Some older children (8y6m–10y8m) discussed their protective strategies for being safe online, whereas younger children did not describe online self-protection awareness or behaviors. These older children commonly used fake identities, modified settings, created more complicated passwords, asked for adults' guidance, and deleted content or apps to protect themselves. For instance, CP08 (8y8m) believed that apps could be "tricked" by providing inaccurate information so the apps would not able to make accurate inferences about them. CP02 (9y0m) described such an approach: *"It [app] can make a mistake [when making an inference about you] because it might, like, you put in a game and be like your uh, 1,000 years old, and then it (the app) thinks you're 1,000 years old."*

Some online self-protective strategies mentioned by most child participants (6y11m–10y8m), were closely related to rules they had learned from various sources (e.g., parents, school, local library, app instructions, online videos). CP02 (9y0m) had learned online safety advice from a game's interface when he first created his account username: *"I just listened to what the things [Roblox interface suggestion] say. It says you shouldn't do that [use your real name as username] When you're making it [username] ... it said in fine script that you shouldn't do it [use your real name as the username]."*

Notably, no child participants considered future risks or consequences from sharing information online. While most of the privacy risks children talked about were related to physical or account threats, children rarely mentioned identity theft or other data breach consequences. No child mentioned any rules they had learned regarding privacy risks from commercial entities [130], or being taught to think critically of why companies might collect their data. CP19 (6y2m) and CP17 (10y4m) mentioned the risk of *"stolen identity,"* with the younger one mimicking what her parents said, possibly without fully understanding it, *"if someone hacked you, then you would be,like, 'Man, I don't care that someone hacked me.' But your mom and dad will be like, 'Oh your identity [will be at risk] or something!' "* In contrast, CP17 (10y4m) could articulate identity risks more clearly, *"I'd be only using part of my name, not my full name, because that's not very safe ... so that they [bad people online] cannot really be like, 'Oh, that's your name.' So that they cannot steal my identity or something."* These examples indicate that children are able to pick up on privacy risks even if they might not fully understand them, and possibly learn more about them as they grow up.

6 DISCUSSION

Consistent with prior literature [20, 65], our findings confirm that children tend to believe that data is static and stored locally rather than understanding data flows or transmissions. Although children in our study recognized that information about them and their activities was stored by apps and platforms, they considered it to be local to their device and were not aware that companies may further use that data to make inferences about them to target ads. Such findings reinforce current evidence that children rarely consider the threats of data collection and profiling by commercial entities [71]. Our findings on children's online self-protective strategies such as hiding real identities [65, 129], giving fake information [65], and deleting apps [127, 129] are consistent with existing research. In addition, as age and child development impact children's privacy perceptions [75], we found that younger children sometimes have more simplistic and incomplete mental models of data processing, privacy risks, and self-protective behaviors than older children.

Our study contributes new findings on the factors shaping children's mental models of data processing as we found that our participants relied heavily on surface-level visual cues to conceptualize how data collection, storage, inferences, and content recommendation work. We provide nuanced insights on children's differing perceptions of data collection and data monitoring purposes – the former serving user convenience and benefiting app companies, the latter ensuring proper app use and safety. We also discovered that children's understanding of data monitoring and tracking was predominantly interpersonal, requiring individual observation (watching through cameras or screens); automated data collection and analysis was not considered. Related, we identified that children's perceived digital privacy risks were also mostly interpersonal (e.g.

bad people, hackers) and that children expected resulting harms to manifest in the physical world.

Based on our findings, we discuss (1) a set of identified factors that appear to influence children's mental models of data processing and digital privacy risk perceptions, and (2) resulting educational, design and public policy implications.

6.1 Factors Influencing Children's Mental Models and Digital Risk Perceptions

Throughout our interviews, children frequently discussed their mental models of data processing, privacy, and digital risks behaviors with reference to several factors that are critical for parents, educators, app companies, and policymakers to consider to better protect children's privacy in digital contexts. These included (1) whether apps provided surface-level visual cues about these processes, (2) whether children had shared certain information explicitly or implicitly during their digital interactions, (3) children's age and development, and (4) children's non-digital experiences.

6.1.1 Surface-level visual cues. Children frequently referred to apps' visual feedback, or described certain aspects of the user interface, to characterize how their data is remembered (e.g., "continue to play" for resuming the game), stored (e.g., app history section), and content recommendations (e.g., "because you watched X, you might like Y"). Conversely, some children seemed to assume that the absence of visual cues in the app meant that no relevant data collection or processing was taking place. Some children believed that exiting or deleting the app would stop data collection or remove the collected data – even if apps continued to run in the background or data remained on backend systems – because closing or deleting the app removed all visual indicators of an app's data collection, processing, or storage.

Our findings relate to and can potentially be explained by research on children's cognitive development. Contrary to older theories which assumed that children are limited to considering only concrete or superficial perceptual cues [92], the past few decades have revealed that by 4 to 5 years of age, children begin to construct implicit "theories" to explain and predict the world around them [120]. These are causal frameworks that are driven by children's interest in understanding why and how observable features link to less-obvious functions, structures, or reasons [46]. Such links may also be related to the concept of "affordance," i.e., the relationship between the perceptual basis (e.g., what does the thing look like) and the inference (e.g., what can the thing do) [42, 43]. In HCI, "affordance" is used to illustrate the operable characteristics in the appearance of an interface [88, 89], which designers need to consider when communicating the meaning of visual cues to users [50].

Whether and how apps use visual cues to communicate with children are critical design choices, as children pick up information through the app interface design and put them together to reason about how data sharing, collection, inferences, and content recommendations work. Our findings highlight the impact of surface cues on children's understanding of data processing and flows, and the potential for children to be misled by intentionally obscured data collection or privacy practices. Children's reliance on surface cues also presents important learning opportunities for children to understand apps' mechanisms.

6.1.2 Children's past data-sharing behaviors. We identified that children's understanding of whether apps could make inferences about them appeared to be associated with their previous data sharing behaviors. Most children in our study described their in-app behavioral data (e.g., the color they choose for their profiles) allowed apps to make inferences about their personal information. Some children also considered that apps' content recommendations were generated based on their prior digital activities (e.g., what types of videos they watched). Children believed that such in-app data-sharing behaviors (behavioral data and direct input data) contributed to apps' knowledge about them. Meanwhile, several children pointed out that apps could not draw conclusions about them because they did not recall providing personal information to the apps. Such findings highlight the need for companies to provide more transparent visual communication in apps to inform children about the presence and function of otherwise hidden data processing mechanisms.

6.1.3 Children's age and development. Consistent with Livingstone's review of child digital privacy research [75], our data likewise suggested that age predicts children's mental models of data processing, online risk perceptions, and self-protection behaviors. Age differences can be characterized roughly in terms of two levels: one is simpler, more naive, and unaware of digital risks, which is largely held by younger children. The other, often held by older children with more mature and skeptical perceptions, shows more awareness of digital privacy risks and corresponding protective actions.

Overall, our younger children primarily identified benefits of data collection (e.g., resuming gameplay, recommended videos). They did not discuss how they could exercise control over data collection. Younger children did not realize that using their real name online could be risky, and they associated negative consequences of exposing one's information mainly with physical threats. In contrast, older children recognized potential negative consequences of data collection, expressing related concerns such as "hackers" getting into their accounts, people finding out where they lived, or companies trying to get them "addicted." Older children seemed to have more elaborate mental models of data processing; for example, they anticipated that they could stop data collection by deleting the collected data in the app or removing the app entirely. In addition, older children considered it unsafe to include their full or partial real name in their username, due to potential physical harms (e.g., somebody might kidnap me) and digital threats (e.g., people hack my account).

As for self-protective behaviors, younger children did not show awareness that they needed to actively protect themselves online, nor did they describe effective self-protective behaviors. In comparison, older children normalized their online self-protective behaviors as a part of their digital experiences and provided various strategies to ensure their online safety.

6.1.4 Children's experiences in the non-digital world. Prior work has pointed out that children translate how they interpret privacy and related governing rules from the analog world [90]. Accordingly,

children in our study described data tracking in an interpersonal manner that occurred on a one-on-one basis, e.g., requiring someone with direct access to what they are doing, such as looking at them through a camera or monitoring their specific account. This is perhaps not surprising, given that children's causal theories are at first developed within a limited number of "core" domains of knowledge (e.g., physics, theory of mind, and biology) [112, 120], and thus conceptual change may be required to understand that the digital world operates on different principles [25].

Our finding that younger children primarily related digital privacy risks to physical threats rather than digital harms indicates that they might be more familiar with physical threats from their non-digital lives (e.g., parents teaching them about "stranger danger"). It is also likely that younger children have not had as many diverse digital experiences as older children, so they may have more limited online risk perceptions.

We also discovered that a few children thought the same ads could not be seen by different people at the same time, or *"if one ad's happening, then maybe it can't happen somewhere else"*(CP17, 10y4m), which may reflect a knowledge transfer from the non-digital world that one object cannot be in two different places at the same time.

6.2 Educational Implication: Expand Digital Education to Include Commercial Privacy at an Early Age

Our findings reveal that the children in our study incorrectly perceived data tracking to be at the one-to-one interpersonal scales, data collection and tracking purposes to be for user convenience, and digital privacy risks to be primarily involving interpersonal interactions online rather than also viewing companies as privacy threats. A common missing piece is that children did not accurately conceptualize companies' role in data processing and were not aware of automated data collection, surveillance and analysis, or the monetary incentives driving surveillance capitalism [130]. This is not particularly surprising. As Laufer and Wolfe [67] pointed out, privacy, being an interpersonal concept, "presupposes the existence of others and the possibility of a relationship with them." Since adults tend to associate privacy in relation to other people rather than viewing digital platforms as privacy threats [15, 49], parents were found to not consider privacy and security conversations necessary until their children become older [65], and digital literacy education for children has focused on interpersonal privacy risks such as cyberbullying and grooming [72] rather than institutional (e.g., data collected by schools and hospitals) or commercial (data collected by companies) privacy risks [70]. Substantially, children have been influenced to primarily conceptualize digital privacy risks at the interpersonal level [70].

Based on our findings, we argue that digital literacy, online privacy, and safety education should be extended beyond the interpersonal level (e.g., hackers or bad characters) to include questions and discussions that gradually help children reach an understanding of what online companies know about them and how such data is used for different purposes. This approach worked well in our interview process and we believe holds potential for educationalx efforts. Specifically, our interview took a gradual approach to ask children what information apps might know and remember about them. Initially, children did not make the connection between the app itself, app companies, and their own in-app behaviors. At the end of the interview, some children were able to put the pieces together and realize that apps or companies know different types of information about them (e.g., age, gender, interests) through collected data.

However, in order for such types of conversations to happen for children at an early age to cultivate their digital risk awareness, it is critical to provide parents the relevant support (e.g., educational materials) to guide their children. For instance, at wellness check-ups, pediatricians can go beyond discussion of "screen time" rules and instead talk about digital footprints, privacy behaviors, and critical awareness of how technology companies try to influence child media use [91]. Some digital risk concepts might not be too difficult to explain. For instance, teaching children to be skeptical of companies' motives, could be similar to teaching them about "stranger danger" – explaining that some apps designed just to manipulate kids to click, like, and watch longer, because that is how apps make money. Families can be encouraged to be choosy about digital products and not simply take "candy" (in-app rewards) from any "strange app" just because it looks shiny and fun.

The use of such analogies to help children conceptualize apps' motives is rooted in the human capacity to engage in analogical reasoning, even in childhood [38, 39]. Analogies involve mapping features or structures from one domain to another, and are involved in a broad swath of reasoning[47, 51, 56, 100]. As prior work has shown, children appear not to consider the commercial aspects of privacy risks and data processing [3, 28, 71]. We argue the need for more thoughtfully designed digital privacy educational materials that include more appropriate and child-friendly use of analogies and metaphors so children can build their reasoning using the "ease of drawing analogies" when comprehending new concepts [109]. For instance, when trying to prepare children for the "digital ocean," instead of primarily focusing on teaching them the skills necessary to stay above water (be safe online), such as wearing life-jackets (virus protection, strong passwords), calling for help (ask parents), and being careful of sharks (bad actors), we should also remind children that every drop of water in the digital ocean is a bit of data. Every time children tap into new areas of water (open new apps), kicking and splashing in the water (do anything online), they generate data flows and waves that are being recorded and analyzed.

Teaching children to watch out for these invisible data flows and waves creates opportunities for them to view the digital ocean with a critical eye, to question the rationality of data collection, and to reflect on their rights (e.g., privacy, free from manipulation) in the digital world [7, 98].

Nonetheless, as Livingstone et al. [74] note, children are a vulnerable population in the digital world. They cannot be expected to fully comprehend the intricacies of the digital data ecosystem when most adults struggle to understand the collection, flow, storage of their data, and the existing data protection laws [15, 59, 93, 126]; or find it hard to make consistent privacy decisions [5]. Better digital literacy education cannot be the only solution. Companies, service providers, and policymakers share the responsibility of protecting children's online privacy.

6.3 Design Implication: Visual Cues for Transparency and User Agency

Our findings suggest that most current apps are not providing sufficient and transparent visual cues and feedback on an app's data flows and processing. Companies like Apple [11] and Google [45] have recognized their responsibilities for family data privacy and are providing learning resources for families' safer device and internet use. Still, neither these nor most other companies clearly explain the commercial side of data use or privacy risks in their user-facing resources, let alone in a way that would be understandable to children. However, helping children – and their parents – better understand privacy implications of using an app should be in a company's interest so as to facilitate trust in the app's privacy protections [82], reduce customer surprise [44, 97], and avoid media outcries [32].

Companies, in particular those developing products aimed at children, need to improve visual cue design of their digital offers to better scaffold children's development of accurate mental models of how an app functions and collects, transfers, and processes data. With thoughtful visual cues and language, children's apps could create proper educational (and visual) experiences as part of their apps that make otherwise hidden digital practices such as data transmission, cloud storage, and profiling more transparent. For instance, imagine a child is saving their progress before exiting a game. When clicking the save button, there could be an animation sending little packets to a cloud while a note pops up, *"your game progress is being saved to our cloud which makes sure we don't forget your data if your tablet runs out of battery."*

While privacy policies are lengthy, difficult to read, and unlikely to be read by anyone [26, 57, 83, 101, 103, 110], in particular children, research shows promise in embedding concise context-relevant privacy notices and controls into the user experience [103–105], such as in the app installation process [17, 63], through audio or visual in-app data indicators [16], or privacy nudges [4, 9]. Similar concepts can be leveraged to help children understand where data is stored, why it is collected, how it is used, and what privacy choices are available to them or their parents.

6.4 Public Policy Implications: Requiring Evidence-based Privacy Transparency and Controls

Our findings reveal that children in our study had a limited understanding of data processing, in particular of automated data collection and analysis, data transmission to cloud backends and third parties, the commercial use of data, and of companies as potential privacy threats. Undoubtedly, children have a lot to learn before they have the competencies to understand what they are consenting to or what they are dealing with when apps are collecting their data. The need to protect children's privacy online has motivated laws, such as COPPA, and provisions to protect children's privacy in the GDPR and the California Consumer Privacy Act (CCPA). While a key component of children privacy regulation has been requiring parental consent for minors – with limited success [35]– the GDPR further requires privacy notices understandable by children if a product processes children's data. However, what that means has been largely left up to the interpretation of companies. What our research shows is that current apps do a poor job at creating transparency about their data practices for children.

Based on our findings we argue that privacy information for children should not be buried in privacy policies but rather needs to be integrated into the actual user experience through improved visual cues and age-appropriate explanations. Importantly, we argue that companies should not only be required to provide age-appropriate notices but should also be required to validate that their notices are indeed understandable by children of targeted age groups. Companies should be required to conduct user testing of such privacy notices and controls with children and publicly document findings. Furthermore, regulators should provide evidence-based guidance and requirements for the design of privacy notices and controls aimed at children, building on our and other research on how children conceptualize data processing and privacy risks.

Furthermore, no children in our study brought up potential future privacy risks of collection and use of their data by companies. Young children have limitations in their sense of "future thinking" [13]. Children who grow up constantly leaving their digital footprints and traces might not realize the implications until years later at which point companies have already compiled and sold multi-year profiles of their evolving interests, personalities, and presumed deficiencies. Privacy harms often manifest as absence of opportunity [6]. Young adults may be disadvantaged or treated unfairly because of their childhood data traces without ever learning about it. We argue that beyond creating transparency about data practices for children, policy makers need to restrict for what purposes data collected about children can be used. Additionally, to prevent future harm, there must be limits for how long data about children can be kept and used to ensure that children's data traces and shared information is kept only for the shortest time necessary to provide the desired service and fully deleted after.

Importantly, for any public policy measures on protecting children privacy to be effective, there needs to be effective enforcement with penalties, which, given children's vulnerable status, should be more severe than those for ordinary privacy infringements and data breaches.

6.5 Limitations and Future Work

When designing the interview protocol, we carefully piloted the materials through multiple iterations with the goal of tailoring the questions to the linguistic and conceptual capacities of young children. However, this was a verbally demanding task, and some younger participants still might have had difficulties either understanding the questions or articulating their answers. Even when children were encouraged to explain their thoughts, they might not have fully understood or may have rushed through the questions. For example, in the closing section of our protocol, designed to assess children's overall understanding of, and attitudes toward, data tracking, collection, sharing, and inference in any of the apps they had used, children used pronouns such as "they" or "it" without specifying to whom they were referring (e.g., "they are watching us" – without clarifying whether it was the hackers, the apps, or the app creators).

Participating families were local to the university so they could visit the research lab for the study session. Because of this, our

sample was geographically and socioeconomically limited. Nearly all the parents in our sample had college or advanced degrees, were employed with white-collar occupations, and were involved in their children's digital media use to some degree (e.g., mediation, rule-setting). As a result, our findings provide a snapshot of a small sample within a particular demographic, and thus it is an open question as to how these results would generalize to larger and more diverse groups of children. Nonetheless, the present qualitative findings still provide a rich and useful in-depth investigation of how a sample of children conceptualize data processing, behavioral tracking and surveillance, and associated privacy risks perceptions.

We anticipate that the observed mental models and gaps in children's understanding would persist in a larger sample, but further research is required to validate and extend these findings. We especially recommend replicating with children from different backgrounds, including more varied socio-economic status, diverse ethnicities, and parents less involved in mediating children's digital activities, as research has shown that families' socioeconomic status and parents' education can influence children's technology understanding [33], media use habits [73], and online safety practices [77]. Meanwhile, neurodivergent children (e.g., those with attention deficit hyperactivity disorder, learning disabilities, or autism spectrum disorder) might understand and reason about data processing and digital risks differently, due to differences in thought processes and digital media use [12, 66]. Furthermore, as we identified that younger children in our study differ from older children in their mental models of data processing, online risk perceptions, and self-protection behaviors, the contrast between "younger" and "older" children here should be treated as relative differences rather than indicating precise age boundaries. Future quantitative research should evaluate the potential transition points involving age, development, and experience that contribute to such differences.

7 CONCLUSION

In our scenario-based interview study with 26 children in the 4–10 age range, we provided deep insights on children's mental models of data processing, behavioral tracking, and privacy perceptions, complementing prior work on children's privacy understanding. Our child participants tended to believe data to be static and stored locally, considered data tracking and monitoring to be possible only on a one-on-one interpersonal basis, mostly associated data collection and tracking with positive purposes and benefits, recognized that their previous in-app behavioral data sharing activities contribute to content recommendation and data inferences, and perceived digital privacy risks as mostly interpersonal rather than considering online companies as privacy threats. We found that such mental models appeared to be influenced by four factors: children's reliance on app's visual surface cues, children's in-app data sharing behaviors, children's age and development, and children's experiences in the non-digital world.

Our findings present opportunities for improved digital literacy education, involving commercial privacy risks. We provide recommendations for designing children's digital experiences with transparent and informative visual cues to empower children's learning, understanding, and competencies in the digital world. Furthermore, policymakers need to create evidence-based guidance for privacy information and controls in products targeting children, limit how children's data can be used and for how long, and properly enforce regulation aimed at protecting children's privacy in the digital world.

ACKNOWLEDGMENTS

This research has been partially funded by a University of Michigan MCubed grant (#9138). We thank Nicole Cuneo and Valerie Umscheid for their research assistance. We are also grateful to all the participating families and the anonymous reviewers for their constructive feedback.

REFERENCES

[1] Council Directive 95/46/EC. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04

[2] Amelia Acker and Leanne Bowler. 2017. What is Your Data Silhouette? Raising Teen Awareness of Their Data Traces in Social Media. In *Proceedings of the 8th International Conference on Social Media I& Society* (Toronto, ON, Canada). Association for Computing Machinery, New York, NY, USA, Article 26, 5 pages. https://doi.org/10.1145/3097286.3097312

[3] Amelia Acker and Leanne Bowler. 2018. Youth data literacy: teen perspectives on data created with social media and mobile devices. In *Proceedings of the 51st Hawaii International Conference on System Sciences*. HICSS, Hawaii, USA.

[4] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, et al. 2017. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)* 50, 3 (2017), 1–41.

[5] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514.

[6] Alessandro Acquisti and Christina Fong. 2020. An experiment in hiring discrimination via online social networks. *Management Science* 66, 3 (2020), 1005–1024.

[7] Susie Alegre. 2020. Data Daemons: Protecting the Child's Right to Dream. https://freedomreport.5rightsfoundation.com/data-daemons-protecting-the-childs-right-to-dream-2

[8] Amelia Alias. 2018. *Children's understanding of online data privacy: a study on Scottish Primary 6 and Primary 7 pupils*. Ph.D. Dissertation. University of Edinburgh.

[9] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your Location Has Been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 787–796. https://doi.org/10.1145/2702123.2702210

[10] Tawfiq Ammari, Priya Kumar, Cliff Lampe, and Sarita Schoenebeck. 2015. Managing Children's Online Identities: How Parents Decide What to Disclose about Their Children Online. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 1895–1904. https://doi.org/10.1145/2702123.2702325

[11] AppleInc. 2020. Families at Apple.com. https://www.apple.com/families/

[12] Thomas Armstrong. 2010. *Neurodiversity: Discovering the extraordinary gifts of autism, ADHD, dyslexia, and other brain differences*. ReadHowYouWant. com, USA.

[13] Cristina M Atance. 2008. Future thinking in young children. *Current Directions in Psychological Science* 17, 4 (2008), 295–298.

[14] Brooke Auxier, Monica Anderson, Andrew Perrin, and Erica Turner. 2020. Parenting Children in the Age of Screens: Parental views about YouTube. https://www.pewresearch.org/internet/2020/07/28/parental-views-about-youtube/

[15] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. 2019. Americans and privacy: Concerned, confused and feeling lack of control over their personal information. *Pew Research Center: Internet, Science & Tech (blog). November* 15 (2019), 2019.

[16] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. 2013. "Little Brothers Watching You": Raising Awareness of Data Leaks on Smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (Newcastle, United Kingdom) *(SOUPS '13)*. Association for Computing

Machinery, New York, NY, USA, Article 12, 11 pages. https://doi.org/10.1145/2501604.2501616

[17] Rebecca Balebako, Florian Schaub, Idris Adjerid, Alessandro Acquisti, and Lorrie Cranor. 2015. The Impact of Timing on the Salience of Smartphone App Privacy Notices. In *Association for Computing Machinery* (Denver, Colorado, USA) *(SPSM '15)*. Association for Computing Machinery, New York, NY, USA, 63–74. https://doi.org/10.1145/2808117.2808119

[18] Carol Margaret 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 (2014), 401–413.

[19] Andrew Besmer and Heather Richter Lipford. 2010. Users' (Mis)Conceptions of Social Applications. In *Proceedings of Graphics Interface 2010* (Ottawa, Ontario, Canada) *(GI '10)*. Canadian Information Processing Society, CAN, 63–70.

[20] Leanne Bowler, Amelia Acker, Wei Jeng, and Yu Chi. 2017. "It lives all around us": Aspects of data literacy in teen's lives. *Proceedings of the Association for Information Science and Technology* 54, 1 (2017), 27–35.

[21] Alex Bowyer, Kyle Montague, Stuart Wheater, Ruth McGovern, Raghu Lingam, and Madeline Balaam. 2018. Understanding the Family Perspective on the Storage, Sharing and Handling of Family Civic Data. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3173574.3173710

[22] Danah Boyd. 2014. *It's complicated: The social lives of networked teens.* Yale University Press, USA.

[23] Danah Boyd, Eszter Hargittai, Jason Schultz, and John Palfrey. 2011. Why Parents Help Their Children Lie to Facebook About Age: Unintended Consequences of the 'Children's Online Privacy Protection Act."'. *First Monday* 16 (10 2011). https://doi.org/10.5210/fm.v16i11.3850

[24] danah boyd and Alice Marwick. 2011. Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies. *A Decade in Internet Time: Symposium on the Internet and Society* 2011 Edi (09 2011), 29.

[25] S Carey. 2009. Oxford series in cognitive development: Vol. 3. The origin of concepts. New York, NY, US: Oxford University Press.

[26] Fred H Cate. 2010. The limits of notice and choice. *IEEE Security & Privacy* 8, 2 (2010), 59–62.

[27] Sangmi Chai, Sharmistha Bagchi-Sen, Claudia Morrell, Raghav Rao, and Shambhu Upadhyaya. 2009. Internet and Online Information Privacy: An Exploratory Study of Preteens and Early Teens. *Professional Communication, IEEE Transactions on* 52 (07 2009), 167 – 182. https://doi.org/10.1109/TPC.2009.2017985

[28] Stéphane Chaudron, ME Beutel, Veronica Donoso Navarrete, M Dreier, Ben Fletcher-Watson, AS Heikkilä, V Kontríková, RV Korkeamäki, S Livingstone, J Marsh, et al. 2015. *Young Children (0-8) and digital technology: A qualitative exploratory study across seven countries.* JRC; ISPRA, Italy, Europe.

[29] Stephane Chaudron, Rosanna Di Gioia, and Mônica Gemo. 2018. Young children (0-8) and digital technology, a qualitative study across Europe. *JRC Science for Policy Report* EUR 29070 EN (2018), 1–266.

[30] Yu Chi, Wei Jeng, Amelia Acker, and Leanne Bowler. 2018. Affective, Behavioral, and Cognitive Aspects of Teen Perspectives on Personal Data in Social Media: A Model of Youth Data Literacy. In *International Conference on Information*. Springer, USA, 442–452. https://doi.org/10.1007/978-3-319-78105-1_49

[31] 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 USENIX Conference on Usable Privacy and Security* (Menlo Park, CA) *(SOUPS '14)*. USENIX Association, USA, 19–35.

[32] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I. Hong. 2018. Breaking! A Typology of Security and Privacy News and How It's Shared. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3173574.3173575

[33] Yang Feng and Wenjing Xie. 2014. Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. *Computers in Human Behavior* 33 (2014), 153–162.

[34] FTC. 2013. Children's Online Privacy Protection Rule. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

[35] FTC. 2020. FTC Gives Final Approval to Settlement with Stalking Apps Developer. https://www.ftc.gov/news-events/press-releases/2020/03/ftc-gives-final-approval-settlement-stalking-apps-developer

[36] GDPR. 2008-08-13. REGULATION (EC) No 765/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93. *OJ* L 218 (2008-08-13), 30–47.

[37] Susan A Gelman, Megan Martinez, Natalie S Davidson, and Nicholaus S Noles. 2018. Developing digital privacy: Children's moral judgments concerning mobile GPS devices. *Child development* 89, 1 (2018), 17–26.

[38] Dedre Gentner. 1983. Structure-mapping: A theoretical framework for analogy. *Cognitive science* 7, 2 (1983), 155–170.

[39] Dedre Gentner and Christian Hoyos. 2017. Analogy and abstraction. *Topics in cognitive science* 9, 3 (2017), 672–693.

[40] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J. LaViola Jr, and Pamela J. Wisniewski. 2018. Safety vs. Surveillance: What Children Have to Say about Mobile Apps for Parental Control. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3173698

[41] Arup Kumar Ghosh, Karla Badillo-Urquiola, Mary Beth Rosson, Heng Xu, John M. Carroll, and Pamela J. Wisniewski. 2018. A Matter of Control or Safety? Examining Parental Use of Technical Monitoring Apps on Teens' Mobile Devices. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3173768

[42] JJ Gibson. 1979. The ecological approach to visual perception. Boston, MA, US.

[43] James J Gibson. 1977. The theory of affordances. Perceiving, Acting and Knowing.

[44] Joshua Gluck, Florian Schaub, Amy Friedman, Hana Habib, Norman Sadeh, Lorrie Faith Cranor, and Yuvraj Agarwal. 2016. How short is too short? Implications of length and framing on the effectiveness of privacy notices. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*. Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016), USA, 321–340.

[45] Google. 2019. Be Internet Awesome. https://beinternetawesome.withgoogle.com/en_us/. Accessed: 2020-08-10.

[46] Alison Gopnik, Laura Schulz, and Laura Elizabeth Schulz. 2007. *Causal learning: Psychology, philosophy, and computation.* Oxford University Press, UK.

[47] Usha Goswami. 1992. *Analogical reasoning in children.* Psychology Press, USA.

[48] Carie Green. 2011. A place of my own: Exploring preschool children's special places in the home environment. *Children Youth and Environments* 21, 2 (2011), 118–144.

[49] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a Low Profile? Technology, Risk and Privacy among Undocumented Immigrants. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3173574.3173688

[50] Rex Hartson. 2003. Cognitive, physical, sensory, and functional affordances in interaction design. *Behaviour & information technology* 22, 5 (2003), 315–338.

[51] David A Hayes and Robert J Tierney. 1982. Developing readers' knowledge through analogy. *Reading Research Quarterly* 17 (1982), 256–280.

[52] Anne K Hickling and Henry M Wellman. 2001. The emergence of children's causal explanations and theories: Evidence from everyday conversation. *Developmental psychology* 37, 5 (2001), 668.

[53] Alexis Hiniker, Kiley Sobel, Ray Hong, Hyewon Suh, India Irish, and Julie Kientz. 2016. Hidden Symbols: How Informal Symbolism in Digital Interfaces Disrupts Usability for Preschoolers. *International Journal of Human-Computer Studies* 90 (03 2016). https://doi.org/10.1016/j.ijhcs.2016.03.006

[54] Donell Holloway, Lelia Green, and Sonia Livingstone. 2013. Zero to eight: Young children and their internet use. *London School of Economics and EU Kids Online* January 2013 Edition (2013), 10–13.

[55] Karen Holtzblatt, Jessamyn Burns Wendell, and Shelley Wood. 2004. *Rapid contextual design: a how-to guide to key techniques for user-centered design.* Elsevier, USA.

[56] Keith J Holyoak, Keith James Holyoak, and Paul Thagard. 1996. *Mental leaps: Analogy in creative thought.* MIT press, USA.

[57] Carlos Jensen and Colin Potts. 2004. Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Vienna, Austria) *(CHI '04)*. Association for Computing Machinery, New York, NY, USA, 471–478. https://doi.org/10.1145/985692.985752

[58] Haiyan Jia, Pamela J. Wisniewski, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2015. Risk-Taking as a Learning Process for Shaping Teen's Online Information Privacy Behaviors. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Vancouver, BC, Canada) *(CSCW '15)*. Association for Computing Machinery, New York, NY, USA, 583–599. https://doi.org/10.1145/2675133.2675287

[59] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere": User Mental Models of the Internet and Implications for Privacy and Security. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)* (Ottawa, Canada) *(SOUPS '15)*. USENIX Association, USA, 39–52.

[60] Deborah Kelemen. 1999. *Beliefs about purpose: On the origins of teleological thought.* Oxford University Press, UK.

[61] Deborah Kelemen. 1999. The scope of teleological thinking in preschool children. *Cognition* 70, 3 (1999), 241–272.

[62] Deborah Kelemen, Maureen A Callanan, Krista Casler, and Deanne R Pérez-Granados. 2005. Why things happen: teleological explanation in parent-child conversations. *Developmental Psychology* 41, 1 (2005), 251.

[63] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as Part of the App Decision-Making Process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI '13)*. Association for Computing Machinery, New York, NY, USA, 3393–3402. https://doi.org/10.1145/2470654.2466466

[64] Angelina KewalRamani, Jijun Zhang, Xiaolei Wang, Amy Rathbun, Lisa Corcoran, Melissa Diliberti, and Jizhi Zhang. 2018. Student Access to Digital Learning Resources outside of the Classroom. *National Center for Education Statistics* NCES 2017-098 (2018), 238.

[65] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L Clegg, and Jessica Vitak. 2017. 'No Telling Passcodes Out Because They're Private' Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–21.

[66] Rebecca Lane and Jenny Radesky. 2019. Digital Media and Autism Spectrum Disorders: Review of Evidence, Theoretical Concerns, and Opportunities for Intervention. *Journal of Developmental & Behavioral Pediatrics* 40, 5 (2019), 364–368.

[67] Robert S Laufer and Maxine Wolfe. 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social Issues* 33, 3 (1977), 22–42.

[68] Jialiu Lin, Shahriyar Amini, Jason I. Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. 2012. Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy through Crowdsourcing. In *UbiComp'12 - Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (Pittsburgh, Pennsylvania) *(UbiComp '12)*. Association for Computing Machinery, New York, NY, USA, 501–510. https://doi.org/10.1145/2370216.2370290

[69] Sonia Livingstone. 2014. Developing social media literacy: How children learn to interpret risky opportunities on social network sites. *Communications* 39, 3 (2014), 283–303.

[70] Sonia Livingstone. 2020. It's none of their business!" Children's understanding of privacy in the platform society. https://freedomreport.5rightsfoundation.com/its-none-of-their-business-childrens-understanding-of-privacy-in-the-platform-society#

[71] Sonia Livingstone and Magdalena Bober. 2004. UK children go online: Surveying the experiences of young people and their parents. *London School of Economics and Political Science* 2004 Edition (2004), 45.

[72] Sonia Livingstone, Julia Davidson, Joanne Bryce, Saqba Batool, Ciaran Haughton, and Anulekha Nandi. 2017. Children's online activities, risks and safety: a literature review by the UKCCIS evidence group. *UK Council for Internet Safety* Oct 2017 Edition (2017), 110.

[73] Sonia Livingstone, Leslie Haddon, Anke Görzig, and Kjartan Ólafsson. 2010. Risks and safety on the internet: the perspective of European children: key findings from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries. *EU Kids Online* 2013 Edition (2010), 2–171.

[74] Sonia Livingstone, Tink Palmer, et al. 2012. Identifying vulnerable children online and what strategies can help them. *UK Safer Internet Centre* 2012 Edition (2012), 2–60.

[75] Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri. 2019. Children's data and privacy online: growing up in a digital age: an evidence review. *London School of Economics and Political Science* 2019 Edition (2019), 2–57.

[76] May O Lwin, Andrea JS Stanaland, and Anthony D Miyazaki. 2008. Protecting children's privacy online: How parental mediation strategies affect website safeguard effectiveness. *Journal of Retailing* 84, 2 (2008), 205–217.

[77] Mary Madden. 2017. Privacy, security, and digital inequality.

[78] Mary Madden, Sandra Cortesi, Urs Gasser, Amanda Lenhart, and Maeve Duggan. 2012. *Parents, Teens, and Online Privacy.* Pew internet & American life project. https://www.pewresearch.org/internet/2012/11/20/parents-teens-and-online-privacy/

[79] Mary Madden, Amanda Lenhart, Sandra Cortesi, and Urs Gasser. 2013. *Teens and mobile apps privacy.* Pew Internet and American Life Project. https://www.pewresearch.org/internet/2013/08/22/teens-and-mobile-apps-privacy/

[80] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355.

[81] Abigail Marsh. 2018. *An Examination of Parenting Strategies for Children's Online Safety.* Ph.D. Dissertation. Carnegie Mellon University.

[82] Kirsten Martin. 2018. The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research* 82 (2018), 103–116.

[83] Aleecia M McDonald and Lorrie Faith Cranor. 2008. The cost of reading privacy policies. *Isjlp* 4 (2008), 543.

[84] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys That Listen: A Study of Parents, Children, and Internet-Connected Toys. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 5197–5207. https://doi.org/10.1145/3025453.3025735

[85] Marisa Meyer, Victoria Adkins, Nalingna Yuan, Heidi M Weeks, Yung-Ju Chang, and Jenny Radesky. 2019. Advertising in young children's apps: A content analysis. *Journal of Developmental & Behavioral Pediatrics* 40, 1 (2019), 32–39.

[86] G. R. Milne, M. Culnan, and Henry Greene. 2006. A Longitudinal Assessment of Online Privacy Notice Readability. *Journal of Public Policy & Marketing* 25 (2006), 238 – 249.

[87] Kathryn C Montgomery, Jeff Chester, and Tijana Milosevic. 2017. Children's privacy in the big data era: Research opportunities. *Pediatrics* 140, Supplement 2 (2017), S117–S121.

[88] Don Norman. 2013. *The design of everyday things: Revised and expanded edition.* Basic books, USA.

[89] Donald A Norman. 1999. Affordance, conventions, and design. *interactions* 6, 3 (1999), 38–43.

[90] Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Faith Cranor. 2018. Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration. *Proceedings on Privacy Enhancing Technologies* 2018, 4 (2018), 5–32.

[91] American Academy of Pediatrics. 2020. Media and Children Communication Toolkit. https://www.aap.org/en-us/advocacy-and-policy/aap-health-initiatives/Pages/Media-and-Children.aspx

[92] Jean Piaget. 1955. The construction of reality in the child. *Journal of Consulting Psychology* 19, 1 (1955), 77.

[93] Emilee Rader, Samantha Hautea, and Anjali Munasinghe. 2020. "I Have a Narrow Thought Process": Constraints on Explanations Connecting Inferences and Self-Perceptions. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, USA, 457–488. https://www.usenix.org/conference/soups2020/presentation/rader

[94] Jenny Radesky, Yolanda Linda Reid Chassiakos, Nusheen Ameenuddin, Dipesh Navsaria, et al. 2020. Digital Advertising to Children. *Pediatrics* 146, 1 (2020), 1–8.

[95] Jenny S Radesky, Jayna Schumacher, and Barry Zuckerman. 2015. Mobile and interactive media use by young children: the good, the bad, and the unknown. *Pediatrics* 135, 1 (2015), 1–3.

[96] Jenny S Radesky, Heidi M Weeks, Rosa Ball, Alexandria Schaller, Samantha Yeo, Joke Durnez, Matthew Tamayo-Rios, Mollie Epstein, Heather Kirkorian, Sarah Coyne, et al. 2020. Young children's use of smartphones and tablets. *Pediatrics* 146 (2020), 1–10.

[97] Ashwini Rao, Florian Schaub, Norman Sadeh, Alessandro Acquisti, and Ruogu Kang. 2016. Expecting the Unexpected: Understanding Mismatched Privacy Expectations Online. In *Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security* (Denver, CO, USA) *(SOUPS '16)*. USENIX Association, USA, 77–96.

[98] General Assembly resolution 44/25. 1989. Article 14 of the UN Convention on the Rights of the Child 1989. https://ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx

[99] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman. 2018. "Won't somebody think of the children?" examining COPPA compliance at scale. *Proceedings on Privacy Enhancing Technologies* 2018, 3 (2018), 63–83.

[100] David E Rumelhart and Donald A Norman. 1981. *Analogical processes in learning.* Technical Report. California Univ., San Diego. Center for Human Information Processing. 335–359 pages.

[101] Norman Sadeh, Alessandro Acquisti, Travis D Breaux, Lorrie Faith Cranor, Aleecia M McDonald, Joel R Reidenberg, Noah A Smith, Fei Liu, N Cameron Russell, Florian Schaub, et al. 2013. *The usable privacy policy project.* Technical Report. Carnegie Mellon University School of Computer Science.

[102] Johnny Saldaña. 2015. *The coding manual for qualitative researchers.* Sage, USA.

[103] Florian Schaub, Rebecca Balebako, and Lorrie Faith Cranor. 2017. Designing Effective Privacy Notices and Controls. *IEEE Internet Computing* 21, 3 (May 2017), 70–77. https://doi.org/10.1109/MIC.2017.75

[104] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. A Design Space for Effective Privacy Notices. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security* (Ottawa, Canada) *(SOUPS '15)*. USENIX Association, USA, 1–17.

[105] Florian Schaub and Lorrie Faith Cranor. 2020. Usable and Useful Privacy Interfaces. In *An Introduction to Privacy for Technology Professionals*, Travis Breaux (Ed.). IAPP, USA, 176–299.

[106] Neil Selwyn and Luci Pangrazio. 2018. Doing data differently? Developing personal data tactics and strategies amongst young mobile media users. *Big Data & Society* 5, 1 (2018), 2053951718765021.

[107] Wonsun Shin, Jisu Huh, and Ronald J Faber. 2012. Tweens' online privacy risks and the role of parental mediation. *Journal of Broadcasting & Electronic Media* 56, 4 (2012), 632–649.

[108] Benjamin Shmueli and Ayelet Blecher-Prigat. 2010. Privacy for children. *Colum. Hum. Rts. L. Rev.* 42 (2010), 759.

[109] Robert Siegler and W. Martha Alibali. 2020. *Children's Thinking*. Pearson, USA.
[110] Daniel J Solove. 2012. Introduction: Privacy self-management and the consent dilemma. *Harv. L. Rev.* 126 (2012), 1880.
[111] Maja Sonne Damkjaer. 2018. *Sharenting = Good Parenting? Four Parental Approaches to Sharenting on Facebook*. Nordicom, USA, 209–218.
[112] Elizabeth S Spelke and Katherine D Kinzler. 2007. Core knowledge. *Developmental science* 10, 1 (2007), 89–96.
[113] Amanda Third, Delphine Bellerose, Juliano DD Oliveira, Girish Lala, and Georgina Theakstone. 2017. Young and Online: Children's perspectives on life in the digital age. *Sydney, Australia: Western Sydney University* 2017 Edition (2017), 1–92.
[114] Patti M Valkenburg, Marina Krcmar, Allerd L Peeters, and Nies M Marseille. 1999. Developing a scale to assess three styles of television mediation:"Instructive mediation,""restrictive mediation," and "social coviewing". *Journal of broadcasting & electronic media* 43, 1 (1999), 52–66.
[115] Patti M Valkenburg, Jessica Taylor Piotrowski, Jo Hermanns, and Rebecca De Leeuw. 2013. Developing and validating the perceived parental media mediation scale: A self-determination perspective. *Human Communication Research* 39, 4 (2013), 445–469.
[116] Simone Van der Hof. 2016. I agree, or do I: a rights-based analysis of the law on children's consent in the digital world. *Wis. Int'l LJ* 34 (2016), 409.
[117] Alexander JAM Van Deursen, Ellen J Helsper, and Rebecca Eynon. 2016. Development and validation of the Internet Skills Scale (ISS). *Information, Communication & Society* 19, 6 (2016), 804–823.
[118] Na Wang, Heng Xu, and Jens Grossklags. 2011. Third-Party Apps on Facebook: Privacy and the Illusion of Control. In *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology* (Cambridge, Massachusetts) *(CHIMIT '11)*. Association for Computing Machinery, New York, NY, USA, Article 4, 10 pages. https://doi.org/10.1145/2076444.2076448
[119] Henry M. Wellman and Susan A. Gelman. 1988. Children's understanding of the nonobvious. *Advances in the psychology of human intelligence* 4 (1988), 99–135.
[120] Henry M Wellman and Susan A Gelman. 1992. Cognitive development: Foundational theories of core domains. *Annual review of psychology* 43, 1 (1992), 337–375.
[121] Pamela Wisniewski, Haiyan Jia, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2015. "Preventative" vs. "Reactive": How Parental Mediation Influences Teens' Social Media Privacy Behaviors. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Vancouver, BC, Canada) *(CSCW '15)*. Association for Computing Machinery, New York, NY, USA, 302–316. https://doi.org/10.1145/2675133.2675293
[122] Pamela Wisniewski, Haiyan Jia, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2015. "Preventative" vs. "Reactive": How Parental Mediation Influences Teens' Social Media Privacy Behaviors. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Vancouver, BC, Canada) *(CSCW '15)*. Association for Computing Machinery, New York, NY, USA, 302–316. https://doi.org/10.1145/2675133.2675293
[123] Pamela Wisniewski, Heng Xu, Mary Beth Rosson, Daniel F. Perkins, and John M. Carroll. 2016. Dear Diary: Teens Reflect on Their Weekly Online Risk Experiences. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 3919–3930. https://doi.org/10.1145/2858036.2858317
[124] Jason C. Yip, Kiley Sobel, Xin Gao, Allison Marie Hishikawa, Alexis Lim, Laura Meng, Romaine Flor Ofiana, Justin Park, and Alexis Hiniker. 2019. Laughing is Scary, but Farting is Cute: A Conceptual Model of Children's Perspectives of Creepy Technologies. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3290605.3300303
[125] Seounmi Youn. 2005. Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach. *Journal of Broadcasting & Electronic Media* 49, 1 (2005), 86–110.
[126] Eric Zeng and Franziska Roesner. 2019. Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and in-Home User Study. In *Proceedings of the 28th USENIX Conference on Security Symposium* (Santa Clara, CA, USA) *(SEC'19)*. USENIX Association, USA, 159–176.
[127] 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 The 15th International Conference on Interaction Design and Children* (Manchester, United Kingdom) *(IDC '16)*. Association for Computing Machinery, New York, NY, USA, 388–399. https://doi.org/10.1145/2930674.2930716
[128] Fangwei Zhao, Serge Egelman, Heidi M Weeks, Niko Kaciroti, Alison L Miller, and Jenny S Radesky. 2020. Data collection practices of mobile applications played by preschool-aged children. *JAMA pediatrics* 174 (2020), e203345–e203345.
[129] Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. 2019. 'I Make up a Silly Name': Understanding Children's Perception of Privacy Risks Online. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300336
[130] Shoshana Zuboff. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: Barack Obama's Books of 2019*. Profile Books, USA.

A HELPER FORM

Hello parent/guardian!

Answering these questions will help us pick the best activities for your child in today's interview session. Leave any questions blank if they do not apply. Thank you so much for your help!

Child's Name or Nickname: _____

What tablet/smartphone type is your child most familiar with? Check one selection.

- Android
- iPad/iPhone (Apple)

What applications on a tablet or smartphone (or other devices such as a Smart TV or Firestick) does your child use in order to watch videos? Circle all that apply.

- Youtube
- Youtube Kids
- Nickelodeon
- Netflix
- Hulu
- Amazon Prime Video
- PBS Kids Video
- DisneyNOW
- Other _____

What tablet or smartphone games does your child play? Check all that apply.

- NBA 2K19 (or other year)
- PBS Kids Games
- Barbie Dreamhouse
- Lego Life
- Tocca Hair Salon 3 (or other Tocca apps)
- Where's My Water
- Candy Crush Saga
- My Talking Tom
- Dr. Panda Town
- Other _____

What applications on a tablet or smartphone does your child use in order to send photos or videos to others? Check all that apply.

- iMessage
- Facebook Messenger Kids
- GroupMe
- Facebook Messenger
- Whatsapp
- Other _____

B INTERVIEW PROTOCOL (ALL SCENARIOS)

INTRODUCTION

Thanks for being here today!

Today we're going to talk about some of the things you do on a phone or tablet, OK? There are no right or wrong answers–we just want to know what you think.

If you don't want to answer a question or need to stop, just let me know and we can stop.

Do you have any questions before we begin? Okay, let's get started!

- What kinds of technology do you usually use?

(If needed): like a smartphone or iPad or game.

- What about game consoles?
- What about computers?
- What about smart home devices (Alexa, Siri, etc.)
- Who owns these? You or somebody else?
- How often do you use the [device identified by child]?

Now I'm going to ask you about three different things that some people like to do with technology. And I want you to tell me if you ever do any of these.

Present child with the three scenario-specific cards.

- Do you ever take pictures on a phone or tablet? (Present the photo card)
- Do you ever play video games on a phone or tablet? (Present the game card)
- Do you ever watch videos or Youtube on a phone or tablet? (Present the video card)

We can start with whichever one you like! Do you want to pick one of the cards to start with? You can even hold onto it if you like!

Child picks one card and proceed to that scenario…

GAME SCENARIO

(If this is the child's second or third scenario during the session, present them with the relevant scenario card to hold onto in order to provide an engaging transition & help mark their progress)

(If the child is repeating herself for the questions you've asked in the previous scenario(s), you can ask if they see any differences of that particular question between the scenarios. E.g. (I know you've told me who made Youtube when we were talking about videos. But for this game, I wonder if you know who made the game? Is it still made by [maker child mentioned earlier]?)

- Do you ever play games on a tablet or smartphone?

[→If yes]

- What games do you like to play?

[→If the child can't come up with the game names, remind them of some popular ones, show icons]

- Have you ever played with one of these [game icons]?

[→If the child mention multiple]

- Which is your favorite one?

[→If child doesn't recognize any of the games we have]:
Skip this scenario

[Once we find a game that the child is familiar with, proceed to open up the game app on the tablet]

- We are not going to play it now, but … when you play the game…
- How does it work?
- What happens next?
- Who made this?

[→If child says I don't know]

- Say "If you were to make a guess …., who do you think made the app?"

[→If the child still doesn't know]

- Ask "Did a person make the game, did a company, or was it both?"
- Did a person make [video app name], did a company, or was it both?

[→person]

- Who are the people, what do they do?

[→company]

- What is a company?
- What do you think the [game] company is or does?
- If you want to learn more about the [game] company, how do you do that?
- Do you think the [company/people] who made [game name] can see what you are doing on the app?

[→If yes]

- How can they do that?
- Why are they doing that?

[→If no]

- Why not?
- How do you feel about that?
- When you play the game, does [game app] remember your progress in the game?

[→If yes]

- How do you think it does that? (remember to follow: you said X, can you explain what that means?)
- Where does the [app name] keep the things it remembers about you? (If the child uses "memories", "brains" etc, we use their words)
- Why does the [app name] keep/remember these things about you?
- Do you think it's okay or not okay that it remembers this? Why or why not?
- Can you delete these memories? How?

[→If no]

- If you turn off the tablet at night and turn it back on the next day, does it still remember?
- How does that work?
- Do you think [game name] knows what kind of games you like or don't like?
- Can you give me an example?
- How do you think [game name] knows that?
- How do you feel about that?
- Do you ever download a new game that it shows you?
- Do you think [game name] shows the same or different games to you than other people?
- Do you think [game name] knows things about you?

- What does [game name] know about you?
- Have you ever seen commercials or ads when you play [game name]?

[→If answer is too short]

- What ads have you seen?
- What do you do when an ad/commercial [use their word] pops up?
- Why do you think there are ads?
- Who put ads in the game?
- Does everybody see/get the same ads?
- Do you tell your friends what games you play?

[→If yes]:

- Why?

[→If no]:

- Why not?
- Do you play with your friends online?
- Do you ever get a new game because your friend told you about it?
- How do you know if the game is okay for you to play on your own?
- Do you tell your parents what games you play?

[→If yes]:

- Why?

[→If no]:

- Why not?
- Do you play with your parents online? Why or why not?

[→If no]:

- See if this at all relates to wanting privacy from parents
- Do you think it's okay or not okay to play games with people you don't know?
- Do you have a username and password to play this game?

[→ If not sure what username is]

- Clarify: Ex. something to log in

[→ If yes]

- What username do you use?
- Is that your real name?

[→If it is the child's real name]:

- Do you ever use just part of your name, for example [give examples based on the child's name: first name only? Initials only?].
- Why or why not?

[→If it's not the child's real name]:

- Why did you choose to use that name?
- Do you only use this name here or in other places too?
- Is it a good idea or a bad idea to use just part of your name, or something that is not your real name? Why?
- When is it safe to use your real name online?

[→ If no]

- Let's say you wanted to set up a username. What name would you use? And why?

[→If it is the child's real name]:

- Would you ever just use just part of your name, for example [give examples based on the child's name: first name only? Initials only?].
- Why or why not?

[→If it is NOT the child's real name]:

- Is it a good idea or a bad idea to use just part of your name, or something that is not your real name? Why?
- When is it safe to use your real name online?
- Do your parents make any rules for you when you play games on a tablet or smartphone?
- What are those rules?
- How do you feel about those rules?
- Why do you think they made those rules?

END

Well, thank you so much, I learned a lot!

Is there anything else about [game app] you want to tell me before we move on?

Do you have any questions for me about [game app]?

*Do you want to*pick another scenario cardand tell me more about it?

VIDEO SCENARIO

(If this is the child's second or third scenario during the session, present them with the relevant scenario card to hold onto in order to provide an engaging transition & help mark their progress)

(If the child is repeating herself for the questions you've asked in the previous scenario(s), you can ask if they see any differences of that particular question between the scenarios. e.g. (I know you've told me who made Youtube when we were talking about videos. But for this game, I wonder if you know who made the game? Is it still made by the maker child mentioned earlier)

- What apps do you use to watch videos online?
- Can you show and tell me how you use [video app name]?
- How do you findvideos to watch?
- How does it work? What happens next?
- How does the video get to [video app name]?
- Who madethis?

[→ don't know]

- If you were to make a guess …., who do you think made the app?

[→ don't know]

- Did a person make [video app name], did a company, or was it both?

[→person]

- Who are the people, what do they do?

[→company]

- What is a company?
- What do you think the [app name] company is or does?
- If you want to learn more about the [App] company, how do you do that?
- Do you think the [company/people] who made [app name] can see what you are doing on the app?

[→If yes]

- How can they do that?

- Why are they doing that?

[→If no]

- Why not?
- Does [app name] rememberwhat you watched?

[→If yes]

- How do you think it does that?
- Where does it keep what it remembers about you?
- If you turn off the tablet at night and turn it back on the next day, does it still remember?
- How does that work?
- If someone else is using the [app name] or tablet, will it still remember what you did?

[→If no]

- Why not?
- Do you think [app name] knows what kind of videos you like or don't like?
- Can you give me an example?
- How does it know that?
- Did it ever show you a video you didn't want to watch?
- Do you think [app name] shows the same or different videos to you and other people?
- Do you think [app name] knows things about you?

[→If yes]

- What does [app name] know about you?
- Have you ever seen commercials or adswhen you watch videos on [app name]?

[→If yes]

- What ads have you seen?
- What do you do when an ad pops up?
- Why do you think there are ads?
- Who put ads in the video app?
- Does everybody see/get the same ads?
- Can your friends look up what you watched on [app NAME]?

[→If yes]

- How?

[→If no]

- Why not?
- Can your friends also see what you've watched on their devices?
- If your friends could see what you watched on [app name], how would you feel about it?
- Do your parents know what you watch on [app]?

[→If no]:

- Why not?
- If your parents could see what you watched on [app name], how would you feel about it?
- What about people you don't know? Is there any way they could find out what videos you watch on [app]?

[→If yes]

- How?

[→If no]:

- Why not?
- How would you feel about it?
- Do your parents make any rules for you when you watch videos on a tablet or smartphone?

[→If yes]

- What are those rules?
- How do you feel about those rules?
- Why do you think they made those rules?
- Do you have a username and password touse the [video app name]?

[→ If not sure what username is]

- Clarify: Ex. something to log in

[→ If yes]

- What username do you use?
- Is that your real name?

[→If it is the child's real name]:

- Do you ever use just part of your name, for example [give examples based on the child's name: first name only? Initials only?].
- Why or why not?

[→If it's not the child's real name]:

- Why did you choose to use that name?
- Do you only use this name here or in other places too?
- Is it a good idea or a bad idea to use just part of your name, or something that is not your real name? Why?
- When is it safe to use your real name online?

[→ If no]

- Let's say you wanted to set up a username. What name would you use? And why?

[→If it is the child's real name]:

- Would you ever just use just part of your name, for example [give examples based on the child's name: first name only? Initials only?].
- Why or why not?
- Is it a good idea or a bad idea to use just part of your name, or something that is not your real name? Why?
- When is it safe to use your real name online?

ENDING

Well, thank you so much, I learned a lot!

Is there anything else about [video app] you want to tell me before we move on?

Do you have any questions for me about [video app]?

*Do you want to*pick another scenario cardand tell me more about it?

PHOTO MESSAGING SCENARIO

(If this is the child's second or third scenario during the session, present them with the relevant scenario card to hold onto in order to provide an engaging transition & help mark their progress)

(If the child is repeating herself for the questions you've asked in the previous scenario(s), you can ask if they see any differences of that particular question between the scenarios. E.g. (I know you've told me who made Youtube when we were talking about videos. But for this

game, I wonder if you know who made the game? Is it still made by [maker child mentioned earlier]?)

- Do you ever share photos you take using a phone or tablet with your friends or family?

[→If yes]:

- What kind of photos do you usually like to share with others?

(Optional):

- Do you ever like to take and share photos of yourself?
- Do you ever like to take and share photos of your things?
- What other kinds of photos do you like to share?
- Are there any kind of photos you don't like to share?
- Why don't you like to share those?

[→If no]: Skip this scenario

- Can you explain how you usually share photos on a tablet/smartphone?

Ask follow up questions to identify an app and understand what the child means about how it works examples:

- How do you like to take photos on a [tablet/smartphone]?
- What is your first step when you want to take and share a photo?
- What happens after that, what do you do next?
- What apps do you use to share photos on a tablet/smartphone?

[→If no app mentioned]: Remind child of some popular ones

- Do you use [ex. iMessage, Facebook Messenger Kids] to share photos?

[→Doesn't know app names]:

- Show child some popular app icons
- Have you ever shared photos with one of these [app icons]?

[→Mentions multiple]:

- Which is your favorite one?

[→Doesn't recognize any]:

- Skip scenario

[→ Identified familiar photo messaging app]

- **Remember app, proceed to take out the tablet**

"Thanks for telling me about how you like to take and share photos on [smartphone/tablet]! I was wondering if you'd like to show me how you do it using this [tablet]. Can you show me how you might take and share a photo?"

[→ Child responds affirmatively]:

- Proceed with the following set of questions.

[→ Child responds negatively]:

- Help the child to find the camera app and guide the child to take the photo.

(Bring out hidden stickers from the box)

- Do you think you could take a picture of one of these things (present choice of stickers)? You can pick which one you'd like to take a photo of, and then you can take it with you back home!
- Can you show me how you do it?
- Looks like the photo is on the [tablet] now. How do you think the tablet keeps this photo?

"Wow, that is an awesome photo! Could you show me how you would share that photo using [mentioned photo messaging app name]? Is it ok for you to share it with me?"

[→If yes]:

- (Interviewer opens up the photo messaging app on the tablet)
- How does it work? What happens next?
- How do you think the app lets you share photos?
- (Walk child through the process of sending photo on the app. RA contact info will be saved on all applications, send designated photo to generic "researcher" contact and be prepared to receive photo on personal device)

[→If no]:

- Why not?
- (Continue to ask the child questions in other modules)

"Ok, I just got the photo! How do you think the photo got from that tablet to my phone?"

- Do you think the photo went anywhere else when you sent it to me?

[→If the child is confused]:

- Did it go through the air on its way to my phone?
- Do you think it's OK for *me* to send this photo to other people?
- What if you don't know those people?
- Why or why not would that be okay?
- What would make it okay for me to share the photo?

[→ don't know]:

- What if I ask for your permission before sending it to someone else?
- Can I send the photo to other people after you leave?
- Why or why not?
- Did a person make [photo messaging app name], did a company, or was it both?

[→person]

- Who are the people, what do they do?

[→company]

- What is a company?
- What do you think the [app name] company is or does?
- If you want to learn more about the [App] company, how do you do that?
- Do you think the [company/people] who made [app name] can see what you are doing on the app?

[→If yes]

- How can they do that?
- Why are they doing that?

[→If no]

- Why not?
- How do you feel about that?
- Does [app/company/maker] remember what you shared?

[→If yes]

- How do you think it does that?
- [Ask clarifying questions]: You said X, can you explain what you mean by that?

- Where does the app keep the photos and other things you shared? Where does it keep the things it remembers about you?
- Will it still remember if someone else uses the app or tablet?
- Do you think it's okay or not okay that it remembers this?
- Why?
- When is it okay to share your photos with other people?
- What kinds of photos are okay for you to share with other people?
- Do you have to be more careful about certain kinds of photos you share?
- Which ones do you have to be more careful about?
- Do you think it is okay or not okay to share your photos with everyone?
- Are there any people that it's not okay to share your photos with?
- What would happen if you shared a photo with someone you didn't know?
- Do your parents have any rules for who you can share your photos with?
- What are those rules?
- How do you feel about those rules?
- Do your parents ever share photos of you with other people?
- Do you like that or do you not like that?
- Why or why not?
- How about your friends, do they share photos of you? Who do they share your photos with?
- Do you think people should ask your permission before they share photos of you?
- Do photos of you belong to you or the person who took the photo?
- Do you ever connect a different [social media] account you use to log into [photo messaging app]?

[→If no]:

- Skip this optional set of questions.

[Offer clarifying examples]: ex. Have you ever connected a Facebook/Google account to use [photo messaging app]?

- Do you think [mentioned social media account] knows what you do in [photo messaging app]?

[→If yes]

- Does [mentioned social media account] use what they know about you from [photo messaging app]? How?
- Is there a way to find out what [mentioned social media account] knows about what you do in [photo messaging app]?

[→If no]

- Why not?
- How does [photo messaging app] connect to [mentioned social media account]?
- Do you like or not like that [photo messaging app] can connect/talk with [mentioned social media account]? Why or why not?
- Why does [photo messaging app] lets you connectto [mentioned social media account] ?
- Do you think [photo messaging app] knows what you do in [mentioned social media account] ?

[→If yes]

- Does [photo messaging app] use what they know about you from [mentioned social media account] ? How?
- What do the [photo messaging app] do with the information it learns from your FB/Google etc.?

END

Well thank you so much, I learned a lot!

Is there anything else about photo sharing or [photo messaging app] you want to tell me before we move on?

Do you have any questions for me about [photo messaging app]?

*Do you want to*pick another scenario cardand tell me more about it?

CLOSING QUESTIONS

Wow thank you so much for all your help so far, I'm really learning a lot from you. We're almost done with the questions I had, do you think it would be okay to ask just a few more questions? You can answer these questions about anything we've talked about today, or anything else you do on a smartphone or tablet at home.

- Do you think apps on smartphones/tablets remember what you did on them or not really?

[→If the child does not provide enough information]

- Refer back to earlier responses from interview [ex. "Remember when I asked you … Whenyou play the game, does [game app] remember your progress in the game?"]
- Do you think the apps can remember what you did even after you're done using them?

[→If yes]

- What does the apps remember?
- What do you think the apps do with the information they remember about you?
- Is it a good or bad thing if the apps remember such things about you?
- What do you think the apps do with the information they remember about you?
- Is it a good or bad thing if the apps remember such things about you?
- Do apps use the information they remember to learn more things about you? (Remind the child again that she could answer the questions from anything that she has seen so far)
- What might an app you use learn about you? What are some of the things it might know about you?
- Would it know what your gender is? (If the child belongs to a binary gender identity, ask "Would it know if you're a boy or a girl?")
- Would it know how old you are?
- Would it know where you live?
- Would it know what you like?
- Would it know what you don't like?
- How do you think the app figures this stuff out?

- What do you think is the thing that's making all these guesses about you?
- Where is this happening?
- Who is doing this?
- Do you think it can make mistakes?
- Why or why not?
- Has an app made a mistake about you before?

[→If yes]:

- Could you tell me more about that time?

[→If no]:

- For example, do you think it might get your age wrong? Could it maybe think you're a different gender?

[→If the child's answer touches on privacy, safety, risk, etc, follow up with below]

- Are there any ways you could stop the app from watching what you're doing?

[→If yes]

- What are some of those ways?
- Have you ever tried to do any of those things before?
- Do you think it's important to learn how to protect yourself when using the apps?

[→If yes]

- Why

[→If no]

- Why not?

C PARENTAL SURVEY QUESTIONS

Thank you for agreeing to participate in our survey. You will be asked questions about your child, you, and your household in general. The survey is estimated to take approximately 15-30 minutes to complete. Your responses will be kept anonymous, and your participation is voluntary. Questions can be skipped or left blank.

(1) Is your child currently attending school (including pre-school)?

- Yes/No/Prefer not to answer

(2) What grade level is your child enrolled in?

- _____

(3) At what age did your child first interact with internet connected devices (smartphones, tablets, etc.)? (Please specify in years)

- _____

(4) Does anyone in your household own any of the following devices (check all that apply)?

- Personal computer
- Regular phone (mobile or landline)
- Smartphone (can access internet, etc.)
- iPad or other tablet devices
- E-reader (e.g., Kindle, Nook, etc.)
- Music Playing Device (iPod, etc.)
- Educational game device (e.g., Leapster Explorer or a V-Smile)
- Console-based gaming system (e.g., Xbox, Nintendo, or Playstation)
- Voice-activated smart speaker (e.g., Alexa/Echo device, Google Home)
- Smart TV that connects to the internet
- Digital media player and microconsole (e.g., Apple TV, Amazon Fire TV)
- Other___
- None of the above
- Prefer not to answer

(5) Does your child own any of the following devices (check all that apply)?

- Personal computer
- Regular phone (mobile or landline)
- Smartphone (can access internet, etc.)
- iPad or other tablet devices
- E-reader (e.g., Kindle, Nook, etc.)
- Music Playing Device (iPod, etc.)
- Educational game device (e.g., Leapster Explorer or a V-Smile)
- Console-based gaming system (e.g., Xbox, Nintendo, or Playstation)
- Voice-activated smart speaker (e.g., Alexa/Echo device, Google Home)
- Smart TV that connects to the internet
- Digital media player and microconsole (e.g., Apple TV, Amazon Fire TV)
- Other___
- None of the above
- Prefer not to answer

(6) Thinking about a typical weekday (Monday-Friday), how much time does your child spend per day using a smartphone or tablet at home?

- Prefer not to answer
- I don't know
- Never
- Less than 30 minutes
- 30 minutes to 1 hour
- 1-2 hours
- 2-3 hours
- 3-4 hours
- 4-5 hours
- More than 5 hours

(7) Thinking about a typical weekend day (Saturday-Sunday), how much time does your child spend per day using a smartphone or tablet at home?

- Prefer not to answer
- I don't know
- Never
- Less than 30 minutes
- 30 minutes to 1 hour
- 1-2 hours
- 2-3 hours
- 3-4 hours
- 4-5 hours

- More than 5 hours

(8) We're interested in whether your child has used a device (e.g., a smartphone, iPod Touch, iPad, or similar smart device) in the last 2 weeks to do any of the following activities. Please indicate the frequency with which they used the device for each purpose in the last 2 weeks.

(Matrix style question with options: Never, less than once a week, about once per week, 2-3 times per week, 4-6 times per week, everyday, several times per day, prefer not to answer, don't know)

- Watch videos/movies
- Use communication apps (calls, texting, video chatting)
- Read electronic books
- Take photos/videos
- Listen to music/audiobooks
- Play games

(9) In the last week, how often did your child use a smartphone or mobile device while falling asleep?

- Never
- Less than once a week
- About once a week
- 2-3 times per week
- 4-6 times per week
- Every night
- Don't know
- Prefer not to answer

(10) [Modified from Valkenburg, P.M., Piotrowski, J.T., Hermanns, J., and Leeuw, R. Developing and Validating the Perceived Parental Media Mediation Scale: A Self-Determination Perspective, Human Communication Research, Volume 39, Issue 4, 1 October 2013, Pages 445–469.]

We are interested in how smartphones and tablets are used in your home. How often do you or other household adults…

(Never, Rarely, Sometimes, Often, Prefer not to Answer, and Not Applicable)

- Watch something together (with your child) on a smartphone or tablet because you both like it?
- Try to help the child understand what s/he sees on an app, game, or video?
- Laugh with the child about the things you see on an app, game, or video?
- Set specific media use hours for your child?
- Watch together because of a common interest in an app, game, or video?
- Point out why some things video characters do are bad?
- Restrict the amount of child smartphone or tablet use?
- Tell your child to turn off the tablet or smartphone when they are watching an unsuitable program?
- Explain what something on an app, game, or video really means?
- Watch or play an app, game, or video together just for fun?
- Explain the motives of digital characters?
- Tell your child in advance the apps they may use, games they may play, or videos they may watch on a smartphone or tablet?
- Watch your favorite program or video together?
- Point out why some things digital characters do are good?
- Forbid your child to use certain apps, games, or videos?

(11) [Mobile Device/Digital Literacy Talk] We are interested in how your family usually uses mobile devices. Thinking about the smartphone(s) or tablet(s) that your child usually uses, how would you describe you and/or your child's use of the device? (Never, rarely, sometimes, often, prefer not to answer)

- We talk about what happens in the videos or games he/she uses, including what the characters are doing and any violence
- Before or after downloading an app, we talk about what permissions the app has requested or what data it might be collecting
- We talk about rules about what videos or apps my child is allowed to use and why
- When there is a design feature that encourages more mobile device usage, such as autoplay, daily rewards, or notifications, I point this out to my child.
- I talk with my child about how to tell whether the information they see in videos, online, or in apps is honest or real.

(12) Who downloads and installs applications to your home devices for your child's use? (Select all that apply)

- Myself or other parent/guardian
- My child
- Child's sibling(s)
- Other people (please describe): _____
- Prefer not to answer
- I don't know

(13) [Modified from Alexander J.A.M. van Deursen, Ellen J. Helsper & Rebecca Eynon. 2016. Development and validation of the Internet Skills Scale (ISS), Information, Communication & Society, 19:6, 804-823.]

For the following questions please select one of the responses.

(Strongly Agree, Agree, Neither Agree nor Disagree, Disagree, Strongly Disagree, Prefer not to Answer):

- I know how to install apps on a mobile device.
- I know how to download apps to my mobile device.
- I know how to keep track of the costs of mobile app use.
- I know which information I should and shouldn't share online.
- I am careful to make my comments and behaviors appropriate to the situation I find myself in online.
- I know when I should and shouldn't share information online.
- I know how to remove friends from my contact lists.
- I know how to change whom I share content with (e.g. friends, friends of friends).
- I know how to open downloaded files.
- I know how to download/save a photo I found online.
- I know how to use shortcut keys.
- I know how to open a new tab in my browser.
- I know how to bookmark a website.

- I find it hard to decide what the best keywords are to use for online searches.
- I find it hard to find a website I visited before.
- I get tired when looking for information online.
- Sometimes I end up on websites without knowing how I got there.
- I find the way in which many websites are designed confusing.

(14) [Modified from Malhotra, N., Kim, S., & Agarwal, J. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research, 15(4), 336-355.]

For the following questions please select one of the responses. (Strongly Agree, Agree, Neither Agree nor Disagree, Disagree, Strongly Disagree, Prefer not to Answer):

- It usually bothers me when online companies ask me for personal information.
- When online companies ask me for personal information, I sometimes think twice before providing it.
- It bothers me to give personal information to so many online companies.
- I'm concerned that online companies are collecting too much personal information about me.
- Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
- Consumer control of personal information lies at the heart of consumer privacy.
- I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.
- Companies seeking information online should disclose the way the data are collected, processed, and used.
- A good consumer online privacy policy should have a clear and conspicuous disclosure.
- It is very important to me that I am aware of and knowledgeable about how my personal information will be used.

(15) What is your age?

_____

(16) I identify my gender as:

- Woman
- Man
- Non-binary
- Prefer not to disclose
- Prefer to self-describe

(17) What is the highest level of education you have completed?

- Some high school
- High school graduate
- Some college
- Bachelor's degree
- Advanced degree
- Trade/Vocational schooling
- Prefer not to answer

(18) I identify my ethnicity as (please select all that apply):

- American Indian or Alaska Native
- Hispanic, Latinx, or Spanish origin
- Caucasian
- Asian
- Black or African American
- Middle Eastern or North African
- Native Hawaiian or Pacific Islander
- Other
- Prefer not to answer

(19) What is your current employment status? Select all that apply.

- Employed
- A student
- A homemaker
- Military
- Retired
- Out of work and looking for work
- Out of work but not looking for work
- Prefer not to answer

(20) Please describe your primary occupation: _____

(21) Would you be interested in being contacted regarding future studies on children's safety online?

- Yes/No/Prefer not to answer

Thank you so much for your time and completion! Your response has been recorded!

D CODEBOOK

Code: Self-protection strategies

Code Values	Definition
Bad characters and their bad behaviors	When children talk about bad people: who are the bad actors, where are the bad actors The things bad actors might do to children, to their account, and to their families. This code also captures children's privacy perception of their account, that they need to protect their account from bad actors like hackers.
Self-protective behaviors from danger or for online safety purpose	What children do to keep themselves safe from all types of danger (bad actors, online threats, risks, bullying, stranger). Include children saying that they would not do/watch something if it's dangerous, or if they will stop doing something if they think it's dangerous or inappropriate.
Risks from exposing one's information	When children explain why they are reluctant to provide personal information(real name, email, address etc). When children explain why they think it's important to protect themselves online due to the risks.
Safety rules and lessons learned from parents, school and other places	When children mention rules about safe app usage behavior or online behaviors learned from various sources like parents, school, library, educational websites etc. If children mention why they choose to follow (or unfollow) or like (or dislike) certain rules. If the rule is not about safety but something else like screen time limit, DO NOT code here.
Strategies to evaluate whether content is appropriate to consume	When children mention they use different evaluation criteria to decide if the content is appropriate for them to consume (whether it's ok to download certain games, play certain games, watch certain videos, etc.) by checking reviews, checking age ratings, asking parents for approval, talking to parents about what he/she watches, watching/playing to find out, other
Other	Code here when other categories do not fit

Code: Personal account(activities) and other stakeholders

Code Values	Definition
Definition of "personal account"	Include children's explanation about their app account, how it works, what the account includes, how they use their account, where the account is, and whether their account is tracked/remembered/known by the app.
Family members' online interactions with me, my account or account activities	When children mention they use their family members' account, family members know about their account, how accounts work among family members, and how children interact with family members when using different app accounts. This code also captures if the child says something about username or password sharing with family members. Also counts if the child doesn't say the word "account" but saying something like "I have my parents in the app as a contact."
Friends' online interactions with me, my account or account activities	When children mention whether their friends know about their account or not, friends can or can't see their account activities, whether they interact with friends online or not. Include both their positive or negative attitudes. Include kids explain how they play with their friends, or the types of interactions they engage in with their friends in the digital world.
Other people's (e.g.,stranger, other online users) view of /interaction with my account and account activities	When children mention whether other people (e.g.,stranger, other online users) know about their account or not, whether other people can or can't see children's account activities, and whether children interact with other people online or not.
Code here when other categories do not fit	

Code: App company and my account

Code Values	Definition
Understanding of app company	When kids answer questions about app companies (including questions such as what a company is, where is it, how it works, who works there, and how you can learn more about the company, or any comments about a company, etc.)

Code: Varying definition of "personal" information

Code Values	Definition
Varying definition of "personal" information	Whenever children mention "personal" or "personal information" and give some sort of examples or explanations of what personal information includes.

Code: Surface cue about how app (features) work

Code Values	Definition
Game apps	When children give a vivid description on how the app works (e.g., things pop up, or you need to tap here for it to go away, etc.)
Video apps	
Photo apps	
Other apps	

Code: Surface cue on how app track/remember your information/data

Code Values	Definition
Game apps	When children give a vivid description of how they learned from visual surface cues regarding how search history, watch history, playing records, other records are remembered or tracked by the app or device. (e.g.,you can tap the "history" menu, there's the "continue to watch" section to tap etc.) Also code when children recall how they interact with the app from memory, and describe it vividly in a visual way.
Video apps	
Photo apps	
Other apps	

Code: Surface cue on app knows your preference for recommended or personalized content

Code Values	Definition
Game apps	When children give a vivid description of how they learned from visual surface cues regarding how apps know your preferences, recommend you new or personalized content (e.g.,the app says "you might like..." or the homepage will have more Minecraft videos).
Video apps	
Photo apps	
Other apps	

Code: Remove surface cue to end the relationship

Code Values	Definition
Remove surface cue to end the relationship	When children mention delete/remove the app, close the app, close the device etc to indicate they don't want to have contact with the apps anymore.—but it has to be very visual description like "you press the delete button." Don't code general mentioning about deletion.

Code: Purpose of data memory/tracking/monitoring/storage

Code Values	Definition
Benefit me	For my benefits, conveniences (e.g., new content recommendation etc.)
Benefit general users/people	When children mention deleting/removing the app, closing the app, closing the device etc. to indicate they don't want to have contact with the apps anymore. Ensure that it is a visual description like "you press the delete button."
Benefit app itself or the company	Improve app service, make apps better, make money etc.
Remember what people did/what people have	This is when children simply say "it remembers what you/people/me/users did" without further expand on concrete benefits. This code also captures if the children says the game remembers what you have in the game: how many coins you have, how many items you've collected.
Negative purpose to people	This includes everyone, people, users, the children him or herself. This code captures when children thinks apps have a negative or harmful purpose such as "get people addicted"
I don't know/unclear	If children say "I don't know" with no follow-up from child/researcher.
Other (Purposes)	Code here when other categories do not fit

Code: Attitude toward apps memory or knowledge of me and my behaviors

Code Values	Definition
Positive (Attitude)	Positive attitude (e.g.,"fine," "ok," also include when app monitoring is ok)
Negative (Attitude)	Negative attitude (also include when app monitoring is not ok)
Neutral (Attitude)	Neutral attitude (e.g.,"don't care," "so-so," "average")
I don't know (Attitude)	When children say "I don't know"
It depends (Attitude)	When children say "it depends" or give both positive example or negative example

Code: Ways that app can or can't monitor/track/watch people

Code Values	Definition
Via people/workers	When children mention about company or apps having people or workers to monitor/watch/track users. Also code if children mention that the lack of people is the reason that no tracking/watching/monitoring occurs.
Via computer/programs/account/software	When children mention that apps or app companies use computer programs/software/account to monitor/watch/track users. Also code if the children says the lack of computer/programs/accounts/software is the reason no tracking/watching/monitoring occurs.
Via camera/screens	When children mention that apps or app companies use cameras/screens to monitor/watch/track users. Also code if the children say the lack of cameras or screens is the reason no tracking/watching/monitoring occurs.
Can't monitor/track people	When children mention that apps or app companies can't monitor/watch/track users in general. This one can be double coded with any of the first 3 sub-codes. For example, if children say "app can't track me because there's no camera" code it both under "can't monitor" and "via camera."
Other (Ways)/unspecified	Code here when other categories do not fit
Don't know/not sure	If children says "I don't know" etc. with no follow-up from child/researcher.

Code: Data memory/tracking storage location

Code Values	Definition
Local storage	When storage is in the iPad, computer, phone, storage bin, local files, local account (when children mention the app doesn't need to connect to the internet to use)
Internet/cloud storage	When the storage is in the cloud, server, internet account, search history, app history
Unspecified (location)	No location is specified.

Code: How I can manage apps' memory (monitor) of me

Code Values	Definition
How I can manage apps' memory (monitor) of me	When children mention the actions they take to manage or influence the way apps remember about them. Examples: "If don't watch it, it will delete the video after 3 months," "If i like or dislike the video"

Code: How app preference work or how apps know my preferences

Code Values	Definition
How app preference work or how apps know my preferences	When children explain how app preference works, or how apps are able to know their preferences. Including comments like, "If I use the app, the app would know that I like the app" or "If I delete the app, the app would know I dislike it"

Code: Preference related to ads

Code Values	Definition
Preference related to ads	When children mention how the app (or ads) know (or show) their preferred types of ads. If you code something here, don't double code it with the "how app preference work" code above.

Code: Gendered view on in-app activities contributing to apps inferences

Code Values	Definition
Gendered view on in-app activities contributing to apps inferences	When children mention the app will know their gender from typical male or female behavior or interests.

Code: How you might influence how apps infer about you

Code Values	Definition
Influence the inferences by providing inaccurate information or show pretended behaviors.	If a typical behavior disproves the norm or deliberately inputting false information (e.g.,a female watching "violent" content, then the app will think you are a male; if you input a different age, the app will think you are of that age).
Inferences are drawn from your in-app behaviors	When children mention how their behavior or inputs influence the app's ability to make inferences about them (e.g.,"you have to tell the app your age or it won't know" or "I need to put in my age for the app to know"). This code also captures when the children mention how they can control what the app infers about them through settings (e.g., enable/allow or disable/deny data access request).
Other	Code here when other categories won't fit.

Code: Different types of inferences

Code Values	Definition
Inference of preference (content, app choice) "First-level" inference of content or preference (e.g.,"it maybe knows what types of videos I like"). You may double code this with the "How app preference work or how apps know my preferences." Include inference of app preference (e.g.,"the apps knows that I like using this app").	
Inference of personal characteristics (gender, age, other hobbies, styles, appearances, skills)	Any inference about personal characteristics. Example: "The app might know that i like to eat ice cream because my username is ice cream 001 or my profile picture is an ice cream."
Inference of name/email	How the app may or may not know your name/email. Example: "The app knows my name (because I gave it to it in the beginning)" "the app knows my email"
Inference related to ads	When children mention how the app makes inferences about you by showing you "personalized ads"
Inference about address or location	How the app may or may not know your address/location. Example: "I don't think it would know where I live"

Code: The thing in the app that makes guesses about you

Code Values	Definition
The thing in the app that makes guesses about you	This code captures if children mention about where/who makes inferences about them occurs/lives.

E LIST OF APPS

Video Streaming Apps

- YouTube Kids
- Nick
- PBS Kids Video
- DisneyNOW
- YouTube
- Amazaon Prime Video
- Hulu
- Netflix

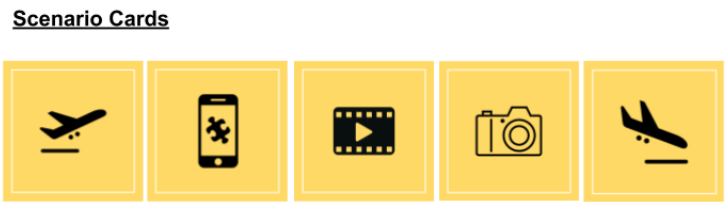
Game Apps

- NBA 2k Mobile Basketball
- PBS KIDS Games
- Barbie Fashion
- LEGO Tower
- Candy Crush
- My Talking Tom
- Where's My Water?
- Toca Hair Salon 3

Messaging Apps

- iMessage
- GroupMe
- WhatsApp Messenger
- Facebook Messenger
- Facebook Kids Messenger

F SCENARIO CARDS



Icon Credits

- Airplane Take Off icon designed by Juan Garces from NounProject. https://thenounproject.com/term/airplane-take-off/59879
- Airplane Landing icon designed by Juan Garces from NounProject. https://thenounproject.com/term/airplane-landing/59877
- Mobile game icon designed by Thays Malcher from NounProject. https://thenounproject.com/term/mobile-game/432812/
- Video icon designed by i cons from NounProject. https://thenounproject.com/term/video/2567868
- Camera icon designed by by Alexander Blagochevsky from NounProject. https://thenounproject.com/term/camera/308298/