Evaluating the Use of Hypothetical 'Would You Rather' Scenarios to Discuss Privacy and Security Concepts with Children

ELANA B. BLINDER, University of Maryland, USA
MARSHINI CHETTY, University of Chicago, USA
JESSICA VITAK, University of Maryland, USA
ZOE TOROK, University of Chicago, USA
SALINA FESSEHAZION, University of Maryland, USA
JASON YIP, University of Washington, USA
JERRY ALLAN FAILS, Boise State University, USA
ELIZABETH BONSIGNORE, University of Maryland, USA
TAMARA CLEGG, University of Maryland, USA

Children are exposed to technology at home and school at very young ages, often using family mobile devices and educational apps. It is therefore critical that they begin learning about privacy and security concepts during their elementary school years, rather than waiting until they are older. Such skills will help children navigate an increasingly connected world and develop agency over their personal data, online interactions, and online security. In this paper, we explore how a simple technique—a "Would Your Rather" (WYR) game involving hypothetical privacy and security scenarios—can support children in working through the nuances of these types of situations and how educators can leverage this approach to support children's privacy and security learning. We conducted three focus groups with 21 children aged 7-12 using the WYR activity and interviewed 13 elementary school teachers about the use of WYR for facilitating privacy and security learning. We found that WYR provided a meaningful opportunity for children to assess privacy and security risks, consider some of the social and emotional aspects of privacy and security dilemmas, and assert their agency in a manner typically unavailable to children in an adult-centric society. Teachers highlighted connections between privacy and security dilemmas and children's social and emotional learning and offered additional insights about using this WYR technique in and beyond their classrooms. Based on these findings, we highlight four opportunities for using WYR to support children in engaging with privacy and security concepts from an early age.

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

Additional Key Words and Phrases: privacy, security, children, learning, curriculum, education

ACM Reference Format:
Elana B. Blinder, Marshini Chetty, Jessica Vitak, Zoe Torok, Salina Fessehazion, Jason Yip, Jerry Allan Fails, Elizabeth Bonsignore, and Tamara Clegg. 2024. Evaluating the Use of Hypothetical 'Would You Rather'

Authors' addresses: Elana B. Blinder, University of Maryland, College Park, MD, USA; Marshini Chetty, University of Chicago, Chicago, IL, USA; Jessica Vitak, University of Maryland, College Park, MD, USA; Zoe Torok, University of Chicago, Chicago, IL, USA; Salina Fessehazion, University of Maryland, College Park, MD, USA; Jason Yip, University of Washington, Seattle, WA, USA; Jerry Allan Fails, Boise State University, Boise, ID, USA; Elizabeth Bonsignore, University of Maryland, College Park, MD, USA; Tamara Clegg, University of Maryland, College Park, MD, USA.

2573-0142/2024/4-ART165
https://doi.org/10.1145/3641004

Scenarios to Discuss Privacy and Security Concepts with Children. *Proc. ACM Hum.-Comput. Interact.* 8, CSCW1, Article 165 (April 2024), 32 pages. https://doi.org/10.1145/3641004

1 INTRODUCTION

The need for age-appropriate learning opportunities about privacy and security to support elementary school children—who typically range between 5-13 years old[1]—in navigating the complexities of online environments has become increasingly important in recent years, given children's expanded use of digital devices and the internet [50]. Children today must navigate numerous privacy and security challenges, such as having their data harvested by apps, assessing the validity of online content, and avoiding inappropriate materials and interactions. In response, there has been a steady growth in the development of digital games [39, 40, 42, 44], videos and presentations [10, 36], and other learning activities [25, 64] aimed at equipping youth with the skills and dispositions required to make thoughtful and informed decisions about managing personal data, engaging responsibly in online interactions, and maintaining online privacy and security. However, most efforts have been aimed at teenagers [26, 58], with less attention paid to younger children, who are forming online media habits and dispositions that they will likely carry into their teenage years and beyond [25, 38, 51].

Providing privacy and security education in a manner that is relevant, meaningful, and accessible for young children also presents unique challenges for adults in a child's life such as parents and teachers. Though some parents may establish rules and expectations [29, 43], many assume these topics will be addressed as a part of their children's formal schooling [29, 32, 38]. Indeed, the topic of online etiquette has been on school librarians' and media specialists' radar for decades [2, 49], with elementary and middle school teachers recognizing the importance of formal classroom instruction in digital literacy, misinformation, and cyberbullying to address incidents involving their students [4, 32, 41]. When it comes to digital privacy and security, however, many elementary school teachers lack confidence about their content expertise and access to age-appropriate curricular resources for their students [4, 32]. Moreover, elementary teachers, who are often responsible for instruction across multiple core content areas, may lack the time, knowledge, or bandwidth to integrate this type of instruction into existing curriculum [31, 32, 38, 53].

Given these realities, many educators resort to the use of reductive, hard-and-fast rules (e.g., lists of technology "do's" and "don't's") to support their students' online safety [5]—a strategy strongly discouraged by the literature insofar as it deprives children of opportunities to explore the nuances of different privacy- and security-related choices [34, 38]. Instead, scholars emphasize the importance of providing privacy and security instruction that is grounded in children's concrete, everyday lived experiences [32] to support their navigation of complex digital risks.

In this paper, we build on prior work by examining how the use of playful, hypothetical dilemmas can foreground children's perceptions and concerns about privacy and security in a manner that may be easily taken up by educators. Our approach in this study specifically emphasizes these types of conversations by presenting scenarios in which there are no "right" or "wrong" answers and in which children are called upon to justify their initial responses and revise them accordingly when new considerations arise through child-adult and child-child discussions. We argue that children stand to benefit from opportunities to think about privacy and security beyond the current constraints of their everyday lives, in which parental and teacher supervision often limits or dictates what choices children can and do make. Such opportunities are necessary if we hope to fully prepare

[1]Most elementary schools in the U.S. are K-5 but in some locations, PreK and/or 6-8th grade are also considered elementary school.

young children for the dilemmas they will face as they grow older and as technology—and associated privacy and security risks—continue to evolve.

One way of doing this is having children work through hypothetical scenarios, such as those posed in a "Would You Rather" (WYR) activity [52], where children are presented with a scenario and two options (e.g., Would you rather eat only pizza or ice cream?) to choose from. Simko et al. [52] used WYR as a co-design technique that "combines design provocations with forced-choice scaffolding" (p. 131), finding the activity useful in playfully "eliciting mental models and values, [and] producing focused yet animated discussions" (p. 131).

Given that privacy and security are nuanced concepts, we aimed to assess the value of using conversations centered around WYR scenarios as a learning tool to support elementary school children in examining how privacy and security related concerns surface in their everyday lived experiences and thinking critically about their priorities and values with respect to these topics.

Specifically, we sought to answer the following research questions:

> **RQ1:** How do children evaluate the pros and cons of hypothetical privacy and security dilemmas?
> **RQ2:** How can educators support children learning about privacy and security concepts through hypothetical dilemmas?

To answer our research questions, we conducted three focus group sessions structured around WYR activities with three different groups of children (N=21) between the ages of 7 and 12 in an informal setting. We then interviewed 13 elementary teachers to gain insight into how this type of hypothetical scenario-based activity could be adapted and expanded to promote rich discussion and learning around digital privacy and security topics in a formal classroom setting.

We found that, when evaluating the relative pros and cons posed by these WYR dilemmas, children attended to three key criteria: the potential for embarrassment, the implications for their personal relationships, and how to 'win' the game and 'cheat the system.' Likewise, we found that children's decision-making was influenced by their family and school rules, surveillance norms, and their mental models of institutional and corporate surveillance. With respect to understanding how educators can support student learning, we observed adult facilitators in an informal learning context scaffolding children's discussions about privacy and security concepts through a combination of modeling complex thought processes, summarizing and elaborating upon children's responses, adding additional criteria to raise the privacy and security related stakes of a scenario, and posing follow-up questions to promote deeper thinking and elaboration. Additionally, our interviews and focus groups with teachers about using WYR in a formal classroom setting revealed connections between privacy and security topics and teachers' instructional priorities in the domain of social emotional learning (SEL). We also identified possibilities for extending this WYR activity to provide more robust learning experiences that go beyond a single experience and/or the classroom context to facilitate school-wide and family-based experiences with privacy and security. Based on these findings, we provide four design opportunities for engaging children in discussions around hypothetical privacy and security dilemmas in classroom settings.

This paper extends prior work on privacy and security learning for children by providing: (1) an expandable set of WYR scenarios and a structure for facilitating privacy and security discussions with elementary school children; (2) evidence that WYR scenarios can elicit children's engagement with complex privacy and security decisions; (3) suggestions for effectively facilitating WYR discussions in formal learning contexts; and (4) suggestions for how this technique can be extended and integrated in a classroom setting to connect with children's social and emotional learning.

2 RELATED WORK

2.1 Children's Privacy and Security Learning Needs

Research suggests elementary-age children are particularly vulnerable to cyber threats, which may be harder to evaluate at their cognitive stage of development [10, 35, 38, 50], owing to their typically limited experience with and developing understanding of privacy threats [65]. Though many young children are comfortable experimenting with new technologies, they may not yet fully comprehend the risks associated with sharing personal information or engaging in other risky behaviors online [37, 56, 59] or when interacting with smart toys and home devices [45]. Tweens (ages 10-12) may be more capable of evaluating the risks associated with a given activity or decision and implementing strategies to reduce or avoid such threats; however, like their younger peers [54, 67], they may have limited awareness of the potential for commercial exploitation of their personal data and how such exploitation may impact them and others in the present and future [1, 53]. For example, in focus groups with tweens and teens, Stoilova et al. [53] observed that youths' mental models of privacy in institutional and commercial contexts were influenced by assumptions carried over from the more familiar domain of interpersonal privacy, often leaving tweens and teens ill-equipped to contemplate how their data-sharing behaviors "might influence their learning, exposure to diversity, choices or decision-making" (p. 201). Furthermore, Sun et al. [54] found that children in preschool through fifth grade construed digital privacy risks and data tracking and monitoring in similar terms, with several employing "one-to-one mode and interpersonal monitoring metaphors" (p. 8), thus calling for more digital privacy learning resources that incorporate developmentally accessible analogies and metaphors. Supporting younger children's speculative reasoning about data privacy and security in this way is crucial especially in the elementary years [29].

Existing cybersecurity education literature primarily focuses on assessing children's knowledge and practices, with less attention paid to the developmental and cognitive factors that may influence children's ability to develop and apply related cybersecurity skills [35, 37]. Elementary age children, who may not yet have the wherewithal to develop and implement their own strategies to mitigate digital privacy and security concerns, often rely upon parents and other adult caretakers for support [29, 61]; however, such approaches pose limitations to children's privacy and security learning. While parental control apps have emerged as a popular way to monitor and limit children's screen time and limit access to "dangerous" content, such approaches deprive children of opportunities to develop agency and relevant skills, while also restricting their opportunities to explore, play, and learn [30, 66]. Moreover, such measures—in the absence of meaningful conversations—can lead to mistrust of parent motives and restrictions [22].

Research has shown that parents often consider privacy and security education as unessential for elementary age children who are not yet using social media [29]. Others opt to discuss the potential consequences of online risky behaviors with their children, but many lack the expertise and/or confidence to help their children develop practical strategies in mitigating these risks, or they may reserve these conversations for the future [22, 29, 30, 37]. Teachers, who frequently observe and are called upon to address a variety of digital privacy and security issues that arise within and beyond their classrooms, report a lack of formal preparation to teach their students about cybersecurity concepts [4, 31, 32, 41].

The absence of established approaches and resources to fill these gaps in parents' and teachers' knowledge render children—who typically receive minimal formal instruction in the domain of digital privacy and security [32, 38]—unequipped with the skills and experience required to identify and negotiate the many privacy and security risks they encounter [37]. These findings highlight the need for learning experiences that are accessible to parents, teachers, and children alike. Our work responds to this need by prompting children to consider and discuss the interrelated nature

of their interactions with their family members, teachers, and peers, and by eliciting feedback from teachers to inform the design and evaluation of privacy and security classroom resources.

2.2 Designing Privacy and Security Learning Approaches for Children

Child-Computer Interaction and privacy and security scholars have explored a variety of approaches toward the study and design of child-facing privacy and security learning tools. Designed educational interventions employed in both informal (e.g., home, after school and summer programs) and formal (e.g., classroom) learning contexts range from videos to interactive stories, digital comics, mobile apps, guided discussions, and game-based learning approaches [35, 50]. Additional techniques demonstrated to support children's privacy and security understanding and skills include storytelling approaches [63] and attention to critical digital literacy skills [66] and data literacy empowerment [1], which can prompt children to question and evaluate privacy-relevant aspects of their everyday lives [66]. In contrast, children may find punitive approaches, which fail to acknowledge the benefits of online activity, unappealing [30].

Prior work has also yielded numerous design recommendations for scaffolding children's (as well as parents' and educators') privacy and security learning. In a study of children's perceptions of "creepy" technologies, researchers developed a set of core questions around the topics of deception, ominous physical appearance, lack of control, mimicry, unpredictability, and relationships that can be used to better understand and support children's developing privacy and security priorities and mental models [61]. Scholars in this domain have also recommended using privacy scenarios related to children's everyday lives, equipping children to learn privacy decision-making skills by considering different contextual norms and nuances and by exposing children to a range of privacy lessons with positive and negative consequences [30]. These authors also emphasize the importance of engaging, developmentally appropriate narratives and characters.

In this paper, we build on prior work through our design and implementation of discussion-based learning opportunities centered around hypothetical scenarios based on real-world dilemmas—though often extreme or fantastical in nature—to support children in thinking through the trade-offs involved in making privacy and security decisions related to aspects of their everyday lives. Our work leverages the affordances of both informal and formal learning contexts by exploring both how playful informal privacy and security discussions among children and adults can promote children's sense of agency [30, 33], and how elementary school teachers envision such a learning activity playing out in their classrooms and across home-school contexts. Finally, the design of our WYR privacy and security learning activity responds to Zhang-Kennedy and Chiasson's [64] call for cybersecurity learning interventions that are easily adaptable (i.e., inexpensive to produce and modify, straightforward, with a low barrier to entry), usable (i.e., easy to understand, efficient to implement, and replayable), and support active and collaborative learning.

2.2.1 Intergenerational Co-Design Techniques Used To Investigate Privacy and Security. Many privacy and security studies in Child-Computer Interaction, like our own, are guided by Druin's Cooperative Inquiry (CI) framework [14, 21]. In CI, children take on roles as users, testers, informants, and/or design partners [15] while engaging in participatory design with adult designers and researchers. Within this context, adult co-designers make concerted efforts to minimize adult-child power dynamics and to build and sustain meaningful inter-generational relationships characterized by mutual trust and understanding, for example, by dressing informally, using first names, engaging in informal conversation during snack time together, and avoiding hand raising and other formal classroom communication norms [14, 18, 21, 62]. Using these techniques, Child-Computer Interaction scholars have explored children's perceptions of parental mobile monitoring technologies [44, 61] and how game-based and storytelling approaches can support children's learning about

online privacy [30]. These studies have yielded insights emphasizing children's acknowledgment of parent control as a form of protection [44, 61], a desire to safeguard these relationships [61], and a desire to understand the connection between privacy and security learning experiences and their everyday lives [30]. Other privacy and security research projects situated in co-design spaces have informed the design of developmentally appropriate learning resources aligned with children's and parents' values and mental models [60, 66].

Also working within the CI framework and most closely related to our study, Simko et al. [52] explored how the forced-choice scaffolding and playful speculative nature of the classic game, Would You Rather (WYR), resulted in sustained and engaging discussions among elementary age children, while "generating formative design insights" (p. 131) for researchers. Though Simko et al.'s research with children incorporated a number of privacy and security-related scenarios, the focus of this research was primarily on understanding WYR as a co-design focus group facilitation technique. Thus, we leverage Simko et al.'s [52] WYR co-design technique, along with recommendations regarding best practices in the design of children's privacy and security learning resources (e.g., [29, 41]), to investigate how discussions centered around hypothetical dilemmas can support children in exploring privacy and security trade-offs and concerns.

2.2.2 School-based Privacy and Security Interventions. Though the literature demonstrates numerous privacy and security concerns associated with the elementary school context and an overall dearth of teacher training and classroom instruction related to these topics [1, 4, 32, 41], few studies are devoted to identifying effective approaches toward privacy and security learning within the context of formal elementary school instruction. Many such efforts are focused on upper elementary and middle school students (between grades four and eight) and their teachers [1, 10, 12, 20, 36, 40, 42], with fewer studies including children and teachers from younger grades. Moreover, the majority of these studies research the efficacy of privacy and security learning interventions solely within lab and/or online environments rather than in authentic classroom settings [64]. Nevertheless, many scholars highlight the importance of teachers' active engagement in the implementation of classroom privacy and security lessons, and subsequently call for their involvement in the design process of classroom-based interventions [23, 41]. Though our research with children in this study took place in informal learning contexts, we respond to this call by engaging teachers in interviews and focus groups to better understand potential obstacles and opportunities presented by WYR as a classroom learning activity.

3 METHODS

To answer our research questions, we developed a series of Would You Rather scenarios related to privacy and security dilemmas children may face in their everyday lives. After obtaining Institutional Review Board (IRB) approval, we ran three remote focus group sessions between December 2021 and March 2022 with a total of 21 children across three established co-design groups to test these scenarios,[2] then conducted interviews with 13 elementary school teachers between March and June 2022 to obtain feedback on their feasibility in classroom settings. All sessions were run over Zoom and recorded.

3.1 Design of the Would You Rather Activity

Leveraging our collective research experience and expertise in privacy and security and childhood education [4, 29, 30, 32–34, 55], five members of the research team collaboratively brainstormed 15

[2]All children had substantial experience participating in online activities on Zoom prior to participating in our online sessions, due to the routines that were established and practiced during their ongoing remote co-design sessions during the pandemic. As a result, children were able to participate with relative autonomy and minimal parent involvement.

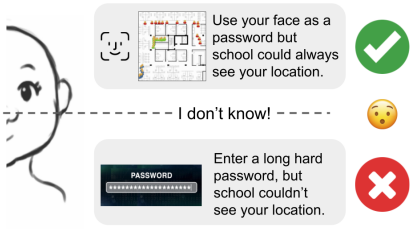
WYR scenarios covering privacy and security topics relevant to elementary-age children's everyday lives (e.g., advertisements, information sharing, online chatting, online identity management, and password management). In developing these scenarios, we approached privacy and security as intertwined concepts, and thus aimed to create scenarios to elicit thoughts on both concepts (even if one topic was foregrounded). For example, Scenario 1 (see Table 1) asked children whether they would rather let a stranger read their diary or give a stranger their house key. This scenario contains implications for both privacy (e.g., with respect to one's personal information and belongings) and security (e.g., with respect to one's physical safety and that of other household members and the safety of their personal belongings). Additionally, we sought to incorporate concrete, non-digital privacy and security concerns likely to be more accessible to younger children (e.g., sharing a house key), while also nudging children toward a consideration of more abstract digital privacy and security concerns (e.g., biometrics and location tracking). After brainstorming, we grouped the scenarios into two overarching categories: (1) passwords & information sharing and (2) advertising & tracking. Each team member then independently ranked scenarios based on which were most relevant to the target group, which were mostly likely to provoke robust privacy and security discussions, and which were the easiest to understand and most appealing for the age range. We then selected the top three ranked scenarios in each category (see Table 1 for the final scenarios and the sessions in which they were discussed).

Though we did not develop a formal framework for assessing the viability of each scenario, our rankings were informed both by our ongoing research in this domain over the past seven years along with the broader body of relevant scholarly literature about children's privacy and security experiences and learning, with which we were already quite familiar.

WYR #	WYR Prompt	Topic Focus	Sessions
1	WYR give a stranger your house key OR let a stranger read your diary?	Information Sharing:Strangers/Intruders	1
2	WYR let a game company read your private online chats OR let your teacher listen to your lunch and recess conversations?	Information Sharing:Corporations/Companies	1,2,3
3	WYR use your face as a password but school could always see your location OR enter a long hard password but school couldn't see your location?	Information Sharing:Passwords	1,2
4	WYR have someone share one of your secrets OR share someone else's secret?	Information Sharing: Personal Data	2,3
5	WYR get a social media account now, but your parents can post info about you on it OR when you turn 13 but only you can post on it?	Advertising/Tracking:Social Media	1,2,3
6	WYR use a tablet with no time limits, but your parents can see everything you do on it OR use a tablet for an hour each day but nobody can see what you do on it?	Advertising/Tracking:Online Activities	1,2,3

Table 1. Would You Rather Prompts showing the privacy and security topic focus for each scenario and in which sessions these prompts were discussed.

(a) WYR#1: Information Sharing: Strangers/Intruders



(b) WYR#3: Information Sharing: Passwords

Fig. 1. Examples of Would You Rather prompt slides for Information Sharing scenarios that were used in remote sessions with children. See Appendix A.1 for complete list.

To accommodate virtual sessions with the children, we created a Google Slide Deck with a separate slide for each scenario (see Figure 1 for example prompts; additional prompts are provided in the Appendix). Each slide included the two response options with icons as visual reminders for developing readers and visual instructions for how to vote. During sessions, facilitators read the scenario, then asked children to vote for the first or second option, or to select "I don't know/It depends." Children could place their hand above or below their head, or at their nose, to indicate their choice or use specified emojis to cast their vote.

During the first session, we were only able to go through five of the six scenarios due to time constraints. Following this session, the team discussed the utility of each prompt, and by consensus prioritized five prompts to show in subsequent sessions, including some used in the first session and one new one from our list. When we observed children struggling to make sense of or connect to a particular aspect of a scenario, we revised the language of the prompt in subsequent sessions. We also modified some scenarios to expand opportunities for entry points to discussion. For example, in our first session, scenarios referenced specific platforms and companies (Instagram, PlayStation); in later sessions, we revised this language using broader terms (social media, game company), given that children might use different platforms.

3.2 Would You Rather Sessions with Children

3.2.1 Procedure and participants. Twenty-one children (ages 7-12) participated in one of our focus group sessions. All were members of one of three longstanding adult-child co-design teams located in different regions of the United States. These teams meet regularly during the school year and children work with internal and external collaborators to address child-centric design problems. Table 2 provides demographic information for each session. Participating children came from three different regions of the country and were diverse in age, gender, and race/ethnicity. Due to the COVID-19 pandemic, all sessions were held on Zoom and lasted approximately 90 minutes.

Children participated primarily through verbal contributions in Zoom, though three participants in the first session participated primarily through text-based contributions using Zoom's chat feature.

Participating adults included each co-design team's program director and university students already working with each co-design-team, in addition to members of our research team. Adults contributed to the facilitation of the session by clarifying scenarios and by posing follow-up questions to children. Sessions included a mix of: (1) question of the day, (2) WYR scenario voting and discussion, and (3) small group discussion. Table 3 provides a breakout of how much time we spent on each activity.

ID#	Age	Gender	RaceEthnicity	Geographic Region	Session Information
K1	8	M	Latin American	Pacific Northwest USA, Urban	Session 1: December 2021; 9 children and 7 adult facilitators
K2	8	M	White / Asian		
K3	8	F	White / Asian		
K4	11	F	White / Asian		
K5	10	M	White / Asian		
K6	8	M	Black		
K7	10	M	White		
K8	9	F	White		
K9	7	F	Black / Asian		
K10	10	M	White / Asian	Northeast USA, Suburban	Session 2: February 2022; 7 children and 8 adult facilitators
K11	10	M	Black		
K12	7	M	White / Asian		
K13	12	F	Black		
K14	11	M	Black		
K15	10	M	Latin American		
K16	7	F	White		
K17	11	F	White	Northwest USA, Urban, Suburban, Rural	Session 3: March 2022; 5 children and 6 adult facilitators
K18	9	M	White		
K19	9	M	White		
K20	12	F	White		
K21	7	M	White / Asian		

Table 2. Child Participant Demographics for the WYR remote sessions.

Activity	Duration	Sessions Included
Question-of-the-Day	10-15 min.	all
WYR Voting and Discussion (4-5 prompts)	60-70 min.	all
Small Group Discussions	15-20 min.	Sessions 2 and 3 only

Table 3. WYR Session Overview showing the structure of activities in each session.

Question of the day. Each session began with a short 'question of the day' warm-up activity, during which each participating child and adult responded to a prompt aimed at introducing the potentially complex and abstract topic of privacy and security in a developmentally accessible way. In Session 1 we asked: 'What kinds of information do you think someone could find about you on the internet?' to get children thinking about their digital privacy and security. In Sessions 2 and 3, we asked: 'What is one thing in your life that you want to keep private?' to prompt children to think more about some of their priorities with respect to their personal privacy. After all participants shared their responses, members of our research team highlighted key takeaways regarding children's expressed priorities and conceptualizations of "privacy," seeking elaboration from children as appropriate.

Individual voting and group discussion of WYR scenarios. Next, participants voted on and discussed 4-5 WYR prompts.

A single prompt was displayed using the screen-sharing feature on Zoom, then read aloud to the group. Children had an opportunity to ask clarifying questions before casting their votes. All children and adults voted simultaneously while a facilitator captured a screenshot of everyone's vote. This screenshot was then added to the session slide deck and displayed during the subsequent discussion. After all votes had been cast, participants were asked to explain why they selected a particular option. Once the discussion began to wane, or in the interest of time, we would introduce a new prompt.

Small group discussions. Following Session 1, we decided to add two small group discussion prompts to Sessions 2 and 3 to observe children's reflections about the privacy and security scenarios posed and how this process might impact their priorities in designing digital tools and environments for others. These discussions were guided by two questions: (1) 'Imagine you are an app designer. What should your app be able to see and share about the people who use it?'; and (2) 'In all of these WYR challenges, your privacy is on the line. Have your thoughts changed about privacy? How?' Though these questions functioned as a starting point for the conversations, facilitators were free to adapt and elaborate upon them to better resonate with the developmental needs and interests of the children in their small groups. Small groups typically consisted of two or three adults and two children, allowing for more intimate and informal conversations. In Zoom breakout rooms, one adult would pose the questions and facilitate a conversation among the children, encouraging them to consider, react to, and build upon each other's responses. Children's responses were captured in a shared digital document and were discussed in a concluding whole group share-out when time permitted.

3.2.2 Data Analysis. The first author reviewed all three sessions' auto-generated Zoom transcripts prior to analysis. We then used MAXQDA software to qualitatively code the transcripts, using iterative, inductive coding [46] and reflexive thematic analysis [6].

Through multiple readings of the transcripts, we identified three overarching codes that mapped onto RQ1 (privacy and security concerns and non-concerns; elaboration: real-life connections; and elaboration: pros, cons, and loopholes), as well as a fourth code aligned with RQ2 (facilitator moves). The first author applied these codes across all three session transcripts, then the full research team met to discuss the excerpts from each code and generate sub-codes for a second round of coding. Once the codebook was finalized, each transcript was re-coded by the first author and emergent findings discussed during weekly team meetings. We then exported excerpts for each of these codes to further analyze, identify trends, and write detailed memos summarizing patterns in the data. Code summaries included any emergent sub-themes and representative participant quotes to describe sub-themes. See Appendix A.3 for the full codebook.

3.3 Teacher Interviews

3.3.1 Procedure and participants. To answer RQ2, we conducted interviews with 13 elementary school teachers at one of our two partner schools (see Table 4). Each session lasted approximately 45 minutes and was conducted remotely on Zoom with 1-3 members of the research team present for each session. We audio and video recorded all the interviews, then transcribed them using Rev.com under a non-disclosure agreement.

In each interview, we shared a selection of our WYR slides and explained how we had implemented the activity with children online. We then invited teachers to discuss their initial reactions to the activity, how they might implement the activity with their own students, the types of resources they would need to support such efforts, ideas about possible modifications and/or extension activities, and their top level concerns regarding privacy and security across children's home and school contexts.

The teachers who participated in our study worked with elementary age students at one of two US schools—a public elementary Pre-K-5 school located in a metropolitan suburb located in the Northeast and a K-8 urban charter school located in the Midwest. The authors have long-term relationships with these schools and worked with their teacher and administrator contacts to recruit teachers from each school. All teachers were invited to participate in a group or individual interview, and all completed consent forms prior to the sessions.

Participating teachers varied in their grade level and content focus, with several teaching across multiple grade levels. These teachers were not necessarily from the same geographic regions as the children in the co-design sessions. The 13 participants included one pre-service (i.e., not yet certified) teacher who identified as male and 12 full-time teachers who identified as female. Teachers who participated in interviews were compensated with a US$30 gift card for their time.

T#	Gender	Grade(s) Taught	Subject(s) Taught	Geographic Region	Interview Type
T1	F	1	Gen. Ed.	Suburban Northeastern Public School, Pre-K-5	Group Interview #1
T2	M	4	Pre-service Teacher		
T3	F	4	Math & Science		
T4	F	4	Reading & Soc. Studies		
T5	F	K-5	Reading		
T6	F	K-5	Vocal Music	Suburban Northeastern Public School, Pre-K-5	Group Interview #2
T7	F	2 and 5	Special Ed.		
T8	F	PreK	Gen. Ed.		
T9	F	K-5	Media Specialist		
T10	F	K	Gen. Ed.	Urban Midwestern Charter School, K-8	Individual Interviews
T11	F	K-8	Spanish		
T12	F	K-8	Counselor		
T13	F	4,5,6	Special Ed.		

Table 4. Teacher Demographics for participants in interviews.

3.3.2 Data Analysis. We followed a similar procedure to analyze the teacher data, using MAXQDA to code transcripts. We developed our initial codebook based on our research question and interview protocol. This resulted in seven codes that captured teachers' responses to the WYR activity as well as additional considerations and extensions to what we proposed (see Appendix Table 6 for full codebook). Two research team members then coded each transcript and exported salient excerpts to facilitate an additional round of thematic analysis, whereby they reviewed excerpts for each code to identify trends, then wrote a detailed memo to summarize patterns in the data. Code summaries included any emergent sub-themes and representative participant quotes to illustrate the sub-themes. We used these code summaries to compare and contrast with the data from the WYR sessions and discussed the emergent themes across both data sets to develop the final set of findings, which we present below.

4 FINDINGS

4.1 RQ1: How do children evaluate the pros and cons of hypothetical privacy and security dilemmas?

The constrained nature of WYR and the absence of any definitive "right" or "wrong" answers opened up participants' perspectives, inspiring children to consider privacy and security situations more expansively. We found that our WYR prompts engendered debate and attention to contextual factors that were especially useful in in eliciting (1) the criteria children prioritized when evaluating hypothetical privacy and security threats and (2) the privacy and security related norms and mental models that influenced their decisions. In this way, our work complements and extends co-design techniques used by Kumar et al. [30], McNally et al. [44], and Badillo et al. [3] by offering a simple approach toward surfacing children's privacy and security concerns.

4.1.1 Children's Criteria for Assessing Privacy and Security Risks. Children frequently referenced three specific criteria when articulating the rationales behind their decisions in relation to our WYR privacy and security scenarios. The two most prominent were the perceived risk of embarrassment

and the implications for their personal relationships. The third criterion was children's consideration of 'winning strategies' (which often involved capitalizing upon loopholes), through which children demonstrated their desire to outsmart the constraints of a WYR dilemma as well as those entities posing a hypothetical threat to their privacy and security.

Emotional concerns: Considering the potential for embarrassment and personal agency. Broadly speaking, the criterion children referenced most frequently in response to the WYR scenarios was the potential for a privacy and security infringement to lead to personal embarrassment. This arose in response to nearly all the WYR prompts posed across the sessions, regardless of age. Specifically, children's consideration of personal embarrassment included their perception of the nature of the exposed information and extent to which their personal agency might be compromised.

With respect to the types of information shared, children tended to focus on the implications of maintaining the privacy of specific content regardless of the form this content took (e.g., text, images, behavior). For example, though most children were relatively unconcerned about having their location tracked by their school or teachers, several expressed strong concerns regarding the privacy of their bathroom activity. Indeed, K8 explained that the first thing she thought of when she heard the word 'privacy' was *"privacy in the bathroom,"* suggesting this was one realm in which privacy and security concerns were already top-of-mind, as echoed in prior research findings [7, 48]. Similarly, when confronted with the prospect of having a private diary accessed by a stranger in WYR#1, K8 expressed a strong desire to maintain the privacy of her diary containing *"super duper secrets,"* whereas children who used their diaries to *"just write how my day was"* (K3) or who deemed their secrets *"not very embarrassing"* (K10, K16) were accordingly less concerned regarding this type of infringement.

Additionally, children expressed concern that a loss of personal control over the public presentation of their skills, behaviors, and image could lead to embarrassment. For example, in his response to the question of the day, K15 shared that he would be embarrassed if someone posted photos of his old drawings, which he felt did not reflect his current level of artistic talent. Similarly, in responding to WYR#4, K12 explained, *"I do a lot of weird things. I don't want my father and mom to send out these weird things with pictures of me,"* while K16 noted she was *"worried about somebody posting something that I don't want posted, like a picture of me with the worst hair style, but they think it's pretty."* Though children often framed these concerns in relation to embarrassment, they rarely speculated about who might be accessing their information or how these entities might judge or shame them. Even when a WYR scenario specified a particular audience, children were often nonchalant about the opinions of others, like what a stranger might think of their private diary (WYR#1) or a large game company about their private correspondence (WYR#2). Rather, children's fears of embarrassment more often suggested a desire for greater agency and control over the dissemination of their personal information regardless of others' opinions, as indicated by K16's comment about her awful hairstyle which others might find pretty. Indeed, K12's discussion of his parents social media sharing practices highlights that children in this age range may already be accustomed to (and frustrated by) adults sharing their personal information without gaining their assent.

Social concerns: Considering implications for others' privacy and security and personal relationships. We observed that the WYR scenarios provided children with opportunities to envision how others could be influenced by their privacy and security decisions. For instance, though many children prioritized their personal privacy with respect to their public presentation, they also frequently voiced concerns regarding inadvertent threats to important people in their lives and their personal relationships with them. They did this both by leveraging knowledge of

their parents' and friends' privacy and security struggles and by considering how their independent choices and actions could impact people close to them.

When children explicitly articulated digital safety consequences, they were often tied to the presumed privacy and security concerns of their parents. For example, several children voiced concerns regarding stolen credit card information and robo-callers—dangers that our young participants were presumably unlikely to directly encounter in their daily lives. Similarly, in responding to WYR#1, K6 referenced his father's experience of having his keys stolen and car broken into, noting that he could apply his father's strategy of changing the locks to prevent future break-ins. Children rarely speculated about the specific privacy and security missteps their parents may have made to enable such breaches, suggesting that the seemingly random nature of these violations may have contributed to their general mistrust of strangers, corporate interests, and online information sharing, a finding we discuss later.

Children did, however, consider how their own privacy and security-related oversights could negatively impact their personal relationships with friends and families. These sentiments came through in K9's reaction to WYR#1—*"If I just gave a random stranger our key, my mom would be so mad! She would never forgive me for that"*—and K20's concern that both of the options in WYR#5 would jeopardize her friendships—*"because you can lose trust both ways. If someone shares your secret, it can become a rumor and you can lose friends. But if you share someone else's secret, you can lose their trust."* Similarly, in a small group discussion, K17 shared that a friend's gaming account had recently been hacked, and explained how this inspired her to be *"a little more careful because I don't want to be hacked and that could also affect other people. Like if I'm playing on my dad's computer or something and it gets hacked, then it could steal his information from work."* A particularly salient example of this phenomenon came from K8's response to WYR#2, in which she suggested that a game company might have the ability to *"hack into your device and send a message to the person you're having a private chat with and say, 'I'm not your friend anymore. Go away',"* or that her private information might be used to get her in trouble with her parents or teachers because, *"if you post the credit card number and they use it, your parents might see it...or your teacher, and they would be like [mimicking an angry voice], 'You weren't supposed to do this!'"*

Though the logic governing K8's theories might strike adults as far-fetched, it reflects our participants' commitment to avoiding disruptions to the stability of their personal relationships within the context of these privacy and security conundrums. Unlike children's discussions regarding the prospect of embarrassment described above, in these instances, the WYR technique showed that children were more inclined to hypothesize about direct consequences tied to specific members of their personal networks (e.g., their parents, friends, and teachers). This may indicate that children possessed a higher degree of prior knowledge regarding these types of privacy and security infringements (due to exposure to parents' experiences) and/or propensity for drawing connections to other more familiar behavioral patterns in their personal relationships (e.g., getting in a fight with a friend, upsetting or disappointing a parent).

'Cheating the system': Considering 'winning' strategies. As in prior research [52], many children were also invested in capitalizing upon loopholes afforded by the playful and hypothetical nature of the WYR scenarios. Given that privacy and security often involves understanding the motives of multiple actors and developing strategies to cope with various threats, thinking through loopholes can help children explore different facets of why privacy and security dilemmas occur and how to overcome certain situations. Our child participants' strategic thinking within this context pointed to a desire to outsmart both those who might pose a risk to their privacy and security as well as the constraints of the WYR game, itself. Moreover, in exercising their ability to bend the conversation toward their immediate interests, children playfully asserted agency over

their learning about privacy and security in a manner that might not be readily available to them in other contexts.

At their best, loopholes represented a playful opportunity for children to engage their imaginations (i.e., coming up with far-fetched scenarios) and critical/argumentative thinking skills (i.e., poking holes in some of the assumptions underlying a scenario). We observed them artfully contorting the criteria and assumptions of the privacy- and security-related WYR scenarios to identify clever ways to achieve a 'win-state' within otherwise undesirable contexts. In our first session, children were especially invested in brainstorming loopholes in response to WYR#1, with K3 suggesting that she could fill her diary with *"secrets that are a lie"* and K6 that he could hand-off his diary to a *"nice stranger"* known by other members of his personal network. Conversations within this context also included hypothetical measures children might take to protect themselves and their home from a stranger's intrusion, for example, by *"jumping down the balcony and locking the door behind them"* (K6), or by screaming in the hopes that someone nearby might call the police (K9). Similarly, K10 and K11's discussion around WYR#4 suggested the central role that devising loopholes played in their general approaches toward navigating an adult-controlled world as children:

> K11: *I would just delete what my mom posts about me… I don't have my dad's password, so I'd just wait until he's using his phone and pretend like I'm downloading something my school sent, but I'd really be deleting the post.*
> Adult facilitator: *Are you saying that you're kind of, like, gaming the system? Like you would choose to have your parents share the account, but then you would just take their phones and delete what they post about you?*
> K10: *It's just to get an account — that is actually smart. Like when kids do something they're not supposed to or figure a way around something, it's not called 'being sneaky'; it's called 'being smart'.*
> K11: *Exactly. Cheating the system.*

In this conversation, K10 and K11 characterized their ability to bend the rules and *"cheat the system"* as a form of intellectual accomplishment, which subsequently granted them agency and control over their personal information and the constraints of the WYR scenario.

In devising hypothetical scenarios in which convenience and privacy were often presented as mutually exclusive, we intended to inspire children's contemplation of the relative affordances and trade-offs associated with each. However, children's propensity for exploiting loopholes could, at times, draw attention away from central privacy and security concepts. In responding to WYR#3, several children expressed that they enjoyed typing out a long complicated password or that they appreciated the potential of this activity to disrupt their school day (e.g., *"If it takes longer, then we're just wasting our time, so nobody will care. We're missing Math!"* (K9)). Though children's schemes to fill their diaries with fake secrets or to seek out trustworthy strangers essentially removed the need to contemplate differences between threats to their family's physical safety and threats to their personal privacy, we argue that these conversational moves nevertheless illuminated children's flexible thinking with respect to the important role contextual nuances play in privacy and security considerations.

4.1.2 Influence of Established Privacy and Security Norms and Mental Models. The rationales children provided in response to their WYR decisions revealed how various privacy and security norms and core belief systems influenced their evaluation of the pros, cons, and trade-offs presented by each hypothetical dilemma. Specifically, children frequently referenced the rules and oversight (or lack thereof) to which they were accustomed in their everyday environments of home and

school, as well as their general suspicion of surveillance employed by corporations and unknown 'hackers.'

Rules, oversight, and surveillance at school and home. A recurring theme that surfaced in WYR discussions was related to children's relative power and agency in an adult-centered society. Within this context, children indicated that they: (1) understood and followed the majority of the rules put in place for them by the adults in their lives; (2) had relatively few opportunities or desires to break these rules due to existing forms of surveillance at home and school; and (3) appreciated the security and protections such rules afforded.

Most children characterized hypothetical acts of surveillance by their teachers, school administrators, and parents as non-concerns and expected that their daily online and offline activities and conversations would be deemed acceptable, unremarkable, and undeserving of reprimand by the adults in their lives. For example, in considering WYR#6, most children—regardless of age—expressed a preference for unlimited screen time accompanied by parent surveillance, indicating that *"there's nothing to hide, so what's the point?"* (K20). The prospect of teacher and school administered surveillance of children's location and peer conversations similarly struck many as relatively inconsequential, with K10 explaining that he didn't *"really care if school sees where I'm going because it's not like I'm going to an ammunition factory or something"* (WYR#3). Though very few children expressed a desire to conceal their online activity from their parents or to engage with forbidden content, one exception was 7-year-old K12, who frequently referenced his desire to *"feel like a spy"* by avoiding all forms of surveillance: *"I don't want a single person watching me. I never think it's good for people to watch me. I wouldn't do it for free candy, or any prize, and not for safety."*

Within this context, children also frequently referenced the existing privileges and forms of parent and school-based surveillance to which they were already accustomed. These norms often functioned to lower the perceived stakes of a given privacy and security-related WYR scenario. For example, children noted that they required teacher permission to leave their classrooms and to visit other school locations, rendering the benefits of avoiding location-tracking in WYR#3 obsolete. Indeed, K2 regarded the suggestion that he could capitalize on additional recess time as preposterous, explaining, *"You can't do that! You just can't do that! I mean you could, but you'd get in trouble because your teacher would just come out. Also, if you stayed outside on the playground, your class would eventually just leave you."* He further illustrated the redundancy of digital location-tracking and flying-under-the radar, by indicating that his school principal already knew every student's name and face. Additionally, in response to WYR#6, several children shared that their family norms already afforded them the privilege of unlimited screen time with few-to-no content restrictions, thereby lowering the stakes of having their online activity monitored by their parents.

Interestingly, many children communicated that they not only accepted, but even encouraged surveillance by the trusted adults in their lives and viewed it as a form of protection against privacy and security threats posed by unknown adults. For example, in discussing the relative advantages and disadvantages of school-enforced location tracking (WYR#3) and conversation surveillance (WYR#2), K11 reasoned, *"if I'm in danger, school would know where I am. So if I get hit by a car or get kidnapped, at least I'm safe."* K15 similarly argued that he wanted his teachers to listen to his recess conversations so they could protect him if he was *"forced to talk to a stranger about something I'm not supposed to hear."* Indeed, some children in our study contemplated the potential repercussions of eliminating existing forms of parent surveillance from their online lives, noting how such an absence might prematurely force them to rely upon skills they were still developing, such as self-discipline and the savviness to avoid content that might negatively impact their mental health. This was apparent in K10's perception that his parents' regulations protected him from harmful overindulgence in violent video games: *"I'd probably see one of my friends playing and then*

be like, 'Oh, I want to play that too.' But I'd rather deal with the consequences than have my attitude change because I'm playing these things. Also, if I had unlimited time, I couldn't get any work done and my life would kind of just be ruined."

Though several children articulated the benefits of surveillance by their parents and teachers, few were inclined to discuss related cons or trade-offs (e.g., a loss of privacy) or question the extent to which these familiar forms of surveillance enhanced their safety. In this regard, these findings suggest that a majority of the children in our study trusted the adults in their lives and had limited experiences involving invasive or unwarranted forms of home and school surveillance.

Perceptions of corporate surveillance and unknown individuals. The overall extent to which children trusted existing forms of oversight, surveillance, and expectations enforced by the adults in their life stood in contrast to their general lack of trust regarding the interests and practices of corporations. Whereas the former were often construed as acts of care and protection, privacy and security breaches imposed by corporate institutions were typically more difficult for children to pin down and were frequently hypothesized as worthy of suspicion and avoidance.

Children expressed concern regarding the motives driving corporate entities' and *"hackers"'* data collection and surveillance practices. In responding to WYR#2, K11 identified corporate interests as tied to financial gains through the theft and sale of his personal data, which he found to be of greater concern than granting his teachers—who presumably lacked such financially driven motives—access to his personal conversations. K13, similarly explained that she was okay with a teacher monitoring her location, but maintained that she would, under no circumstances, grant an app like TikTok access to this same information. Though invested in protecting her personal information from corporate interests, K13—like many other children who hypothesized about the *"really weird and sketchy stuff"* (K19) a company might do—did not fully articulate what she thought TikTok would do with her data or how this might directly impact her in the present or future.

Additionally, children expressed concern about the potential scale of surveillance with larger corporate entities. For example, K1 attended to questions regarding the *amount of individuals accessing his data*, arguing that surveillance by a single teacher would be safer, while K7 suggested that the total *amount of data* to which a game company had access was more significant, as it would render his personal *"one little kid"* data relatively invisible and unimportant.

4.2 RQ2: How can educators support children learning about privacy and security concepts through hypothetical dilemmas?

To understand how nuanced conversations around hypothetical privacy and security dilemmas can used in classroom contexts, we analyzed both the techniques adult facilitators used to nudge children toward a deeper contemplation of privacy and security considerations and the recommendations elementary teachers made for implementing the WYR technique in a formal classroom learning environment. We found that: (1) adults in the co-design groups took a flexible approach toward facilitating discussions around the WYR privacy and security scenarios; and (2) classroom teachers emphasized connections between hypothetical privacy and security dilemmas and students' social emotional learning curriculum and felt that the activity could be extended in a variety of ways.

4.2.1 Educator Approaches in Informal Learning Contexts. Within the informal co-design learning contexts in which we implemented our privacy and security WYR sessions, we observed adult co-facilitators scaffolding children's discussions about privacy and security concepts through a combination of: (1) modeling complex thought processes; (2) summarizing and elaborating upon children's responses; (3) adding additional criteria to raise the stakes of a scenario; (4) and posing follow-up questions to promote deeper thinking and elaboration. We describe each strategy in more detail below.

True to cooperative inquiry techniques [18], adult facilitators participated in design activities (e.g., voting) and would occasionally model the thought processes that informed their decisions by highlighting the underlying implications of an option and openly displaying uncertainty due to the complexity of a given scenario. For example, in response to WYR#5, an adult facilitator shared how the ethical and interpersonal dimensions of the scenario made it difficult for her to choose one option over the other: *"I chose 'I don't know' because I feel... I guess I didn't really want to share anybody else's secrets and I want to be a faithful friend. But I don't want somebody else to break my trust either."* This reflection highlighted how the privacy and security dilemma could impact interpersonal relationships—a consideration which had not yet been directly raised by children in the discussion, who had been more focused on the nature of their secrets. Additionally adult facilitators often summarized, synthesized, and elaborated upon child responses: *"K1 raises an interesting question. A video game company could be like hundreds of people looking at your chat. But K5 said 'those websites and apps could be sued,' so he's also thinking about laws."*

When child attention strayed from the core privacy and security aspects of a scenario, adult facilitators often introduced new scenario criteria to up the ante and redirect conversation back toward the intended learning content. For example, when K10 explained his lack of concern about his parents monitoring his online activity since he wouldn't be doing anything controversial, an adult facilitator asked him to consider a situation in which he might need or want to engage in an online activity of which his parents might disapprove and how this may or may not impact his response to WYR #6. Similarly, facilitators posed follow-up questions to prompt deeper thinking and elaboration, such as, *"Does it matter if your family is in your house when you handover the key? Or what if they're on vacation?"* (WYR #1) and, *"Is it more about your control and your power or is it that you're afraid your parents will post something embarrassing?"* (WYR #4).

These findings highlight the overall flexible nature of adults' approaches toward facilitating discussions around these privacy and security WYR scenarios. These interventions were not scripted, but arose naturally in response to the ideas and perspectives raised by children in the moment. At the same time, these facilitator moves functioned to carve out additional space for children to expand upon and rethink their initial rationales in a manner that acknowledged the complexity of each scenario and of privacy and security decisions more broadly.

4.2.2 Educator Perspectives on Classroom Implementation. The teachers with whom we spoke responded favorably to the privacy and security related WYR activities we shared and felt that some or all of the questions were relevant, appropriately thought-provoking, and developmentally accessible for their students. Teachers felt that the WYR activity structure would be similarly engaging for students across grade levels, with several teachers noting that they were already using WYR activities in their classrooms. Teachers additionally discussed some of the top-level privacy and security topics they deemed most important for their students, which included password sharing, media consumption through TikTok and YouTube, online exploitation and maintaining the privacy of personal information, and issues of consent when video recording and/or sharing peers' information online. Though teachers stressed the importance of scenarios kids could relate to (particularly in the younger grades), they did not always agree on what these should be. Some teachers felt questions about social media could be relevant for all ages; others felt they primarily applied to upper elementary and/or middle school students. Teachers who worked with younger grades suggested additional questions around privacy and security focused on the concept of strangers, YouTube, TikTok, and Roblox. Below we discuss some of teachers' key insights with respect to implementing discussions around constrained hypothetical privacy and security related dilemmas in an elementary classroom setting, namely their consideration of: (1) the connections between privacy and security education and students' social emotional learning needs; and (2)

opportunities to enhance student learning by building upon and extending students' discussions around hypothetical privacy and security dilemmas.

Privacy, security, and students' social emotional learning (SEL) needs. Social Emotional Learning (SEL)—also referred to as character education, 21st-century and/or soft skill development—involves learning experiences designed to support children's ability to understand and manage their emotions and to effectively interact and communicate with others [17, 28]. Teachers at both schools said the WYR activities could fit into their SEL curriculum. They observed connections between privacy and security topics and the types of learning goals pursued by school guidance counselors, with T3 noting that, *"This could easily be SEL, because those are things that matter to the kids—that house key and so forth—that affect them personally."* T7 similarly observed that WYR#5 presented *"a plethora of different things in the social emotional realm with trust and who you trust and being a loyal friend."* Additionally, T12, a multi-grade guidance counselor, noted how our privacy and security WYR questions might be used as a launching pad to discuss the emotional implications of children's online experiences and decisions. She, like many of the general and special education teachers with whom we spoke, felt it would be beneficial to emphasize the connections between privacy and security quandaries and students' emotional health and well-being: *"If I was talking about cyber bullying or something was posted and maybe it was body shaming or someone didn't like your post, my role would be dealing with how it affects your self esteem and the emotions behind the post—what did you feel when you saw that post or when you saw something on TikTok that was inappropriate?"*

Teachers also considered the potential socio-emotional impacts their students' may experience as a result of engaging in these types of privacy and security discussions. Several emphasized the importance of keeping scenarios simple and focused and cautioned against posing too many at a time because they sensed certain questions could be anxiety-inducing for some students. T3 noted the very personal nature of some of the questions, explaining, *"The content pulled me back at first because some of it's pretty personal. My students do Would you Rather all the time, but the content, like, would you give them a house key? Wow. That's pretty powerful."* T6 emphasized the importance of carefully considering how to prevent students from feeling overwhelmed by designing lessons to help children connect their WYR decisions to deeper learning goals. She also suggested that the multitude of possible considerations and loopholes a student might contemplate in response to a WYR scenario could *"spin out of control and maybe even cause anxiety in some kids,"* and suggested children who felt overwhelmed might *"not necessarily even think it through, but just kind of pick without deep thoughts and conversation."*

Teachers' attention to the feelings children might experience in these contexts highlights the significance of the emotional aspects of privacy and security, an approach which has traditionally been less of a focus in the literature on children's privacy and security education.

Proposed extensions. Teachers viewed privacy- and security-related WYR activities as an engaging and useful warm-up activity within the context of a broader lesson and were eager to consider where they might go from there. Though some saw WYR as a quick activity they could implement on an as-needed basis, many considered possible extension activities that could be designed to build off our WYR examples to create a more well-rounded learning experience for their students. Some teachers recommended incorporating fictional narratives into children's privacy and security instruction, either by exploring dilemmas and themes in stories with which students' were already familiar (e.g., fairy tales, Harry Potter, World of Warcraft) or through the introduction of new read-aloud stories. Some teachers also noted benefits of having children develop their own privacy- and security-related WYR scenarios within the context of a fictional environment, an

approach that aligns with the child participatory design techniques of fictional inquiry [18] and speculative design [13]:

> *"Perhaps have them create their own activities and rules.... This is the forest and, if we cross this line, you're going into caves or places that are perhaps not so safe. Maybe there are bears and creatures that are predators. So using that analogy, how could you make this a safe place for the people that want to visit?"* (T11)

Additionally, several teachers recommended adding drawing and/or writing prompts (depending on their students' grade level) that could be completed as part of children's independent practice at school or as homework, with their families.

Echoing the principles of Connected Learning [24], teachers also considered how to extend privacy and security WYR discussions beyond their individual classrooms to engender connections between students' home and school contexts and to make privacy and security a unifying theme across their entire school community. Several noted the importance of sending home a letter to ensure that parents understood the purpose of the activities and potentially controversial nature of the questions, with T6 joking, *"When the kid comes home and says, 'We talked about whether or not I should give away my house key,' it's like—'uh-oh.'"* Additionally, teachers recommended activities to educate parents about privacy and security topics. Some of these included homework assignments for children to *"teach their parents"* and/or to complete an activity together. Others included relevant literature, discussion guides, or directly engaging parents in privacy and security related WYR activities about their children *"so that we can have some type of global connection with the house and the family, and so that they know that we are here as a support system"* (T11). In addition to generating ideas to foster home-school connections in the area of digital privacy and security, some teachers also considered school wide initiatives that could extend and reinforce classroom-based learning experiences, such as a whole school cyber safety week or incorporating WYR scenarios into the principal's daily announcements.

These findings indicate teachers' interest in a holistic approach to privacy and security education that both acknowledges the emotional aspects of these topics as well as the connected nature of children's lived experiences across the classroom, school community, and home contexts. Rather than silo-ing this learning content within the confines of an individual lesson or unit, teachers shared their vision for fostering a broader learning infrastructure to support children, teachers, and families in considering privacy and security issues.

5 DISCUSSION

In this section, we synthesize our findings as they relate to: (1) what the WYR activity revealed about children's perspectives and their abilities to grapple with and expand upon a wide variety of privacy and security related dilemmas; and (2) how WYR activities and adult-facilitated discussions may not only enhance privacy and security education for children, but also open up opportunities to develop their socio-emotional skills and resilience. Our analysis surfaced four key opportunities for enhancing children's privacy and security education through the incorporation of hypothetical dilemmas. We discuss these opportunities below, followed by a discussion of our study's limitations and recommendations for future work.

5.1 Opportunities for Enhancing Elementary Privacy and Security Education through the Incorporation of Hypothetical Dilemmas and Beyond

Though our initial intent in undertaking this study was to better understand and address challenges associated with engaging younger children in privacy and security related discussions, our research findings raise four key opportunities for enhancing elementary privacy and security education in

formal classroom settings: (1) understanding and capitalizing upon students' unique experiences, values, beliefs, and interests; (2) promoting student engagement and agency through playful speculative discussions; (3) supporting teachers' knowledge and practices through flexible conversation and learning tools; and (4) highlighting the social and emotional aspects of privacy and security learning. Though the literature rightly calls for interventions to further develop middle school and high school age students' critical understanding of information flows (how their personal data are collected, used, processed) and the personal and broader societal implications of these processes [1, 31, 56], our findings point to several avenues through which to build an early foundation capable of supporting such endeavors. In the sections which follow, we describe and discuss the implications and the design recommendations associated with each of these four opportunities.

5.1.1 Opportunity 1: Understanding and Capitalizing upon Students' Unique Experiences, Values, Beliefs, and Interests. Consistent with Simko et al. [52], our implementation of this WYR technique helped us understand children's priorities, norms, and mental models. In so doing, it also surfaced and prompted us to reconsider some of our underlying assumptions about children's privacy and security values and lived experiences (e.g., that children would have a stronger desire for autonomy and freedom from surveillance and rules). In their 5D framework for preteen's privacy education, Kumar and Byrne [31]—drawing on Freire's work [19]—call for an *emancipatory learning* approach to privacy that *"requires adults to respect and build upon preteens' existing privacy-related knowledge and experience"* (p. 11). We build on this literature by demonstrating how such an approach is both feasible and equally relevant to the privacy and security education of younger children, whose experiences and concerns are plentiful, albeit somewhat different from those of their slightly older peers. Rather than looking for gaps in children's knowledge, we assert that this discussion-based WYR activity can serve as a valuable informal formative assessment to help teachers (as well as researchers) capitalize upon a community of students' assets and prior knowledge with respect to privacy and security. The knowledge derived from such an approach can, in turn, inform the modification and development of additional privacy and security dilemmas and other learning activities likely to resonate with a target child audience.

During our WYR discussions with children, this work was often enacted by session facilitators (many of whom had long standing relationships with the children in their intergenerational co-design teams) whose on-the-fly modifications often spoke to their substantial knowledge about their young teammates' everyday lives. Similarly, the teachers with whom we spoke called attention to important considerations which we, ourselves, could not have anticipated, such as their students' socio-emotional and academic needs along with tried-and-true methods for raising sensitive topics. These insights highlight the importance of going beyond standardized one-size-fits-all privacy and security curricular approaches to create customizable structures and content that can be meaningfully informed by students' evolving experiences and concerns. Thus, we argue that elementary teachers, who often spend a majority of their school day working with a single core class of students, are uniquely positioned to understand and leverage their students' specific needs and interests—both within and beyond the domain of privacy and security education—when designing or modifying learning activities.

5.1.2 Opportunity 2: Promoting Student Engagement and Agency through Playful Speculative Discussions. In addition to providing insights about children's priorities, norms, and mental models, our findings indicate that children's participation in conversations around hypothetical privacy and security dilemmas can serve as an engaging and empowering learning opportunity. The WYR technique incorporates learning approaches that are both collaborative (i.e., incorporating discussion and mediation between learners) and active (i.e., incorporating consistent interaction and feedback), as recommended by Zhang-Kennedy and Chiasson [64] for the design of cybersecurity

learning tools. This was evident, for example, in the manner in which K10, K11, and an adult facilitator riffed off each other and co-constructed their understanding of *"cheating the system,"* and during the many occasions in which adult facilitators summarized, elaborated upon, and posed questions about children's responses. Within this context, children's active learning—also referred to as *learning-by-doing* [11, 64]—involved the very acts of weighing pros, cons, and considering a myriad of related consequences that comprise the types of privacy and security thinking and 'doing' through which children in this age range are most likely to benefit [32, 38].

Though we found children's devotion to exploring loopholes could, at times, steer conversation away from core privacy and security content, we argue that, by re-envisioning and re-inventing the assumed confines of these hypothetical scenarios, children enacted the types of flexible thinking and attention to context demanded of real world privacy and security related decisions. Therefore, while the content of our WYR scenarios and children's strategies could, at times, be somewhat outlandish, the nature of the activity set them up to engage with authentic privacy and security debates in a manner that was fun and accessible. Thus, we recommend an emphasis on the acceptance and navigation of ambiguity when it comes to children's privacy and security education, as opposed to attempts to develop or identify definitive right or wrong answers. For example, the simple option of an *"I don't know/It depends"* response may support children in recognizing and articulating the complexity and nuance of a privacy and security dilemma.

Additionally we argue that the hypothetical and design fiction nature of this low-tech activity, which builds upon prior research on involving children in speculative design [9, 13, 57], can offer children an opportunity to transcend and critically consider the constraints governing their everyday lives—to 'cheat the system,' devise creative loopholes, and temporarily embody the perspectives and concerns of adults. We believe such an approach is particularly well-suited to elementary-age children who, as indicated by our findings and others' [38], can be accustomed to a fair amount of adult oversight of their online activities. Thus, our findings suggest that providing children with a level of agency and autonomy uncharacteristic of their daily lives may help them build their privacy and security reasoning skills and confidence before tackling higher stakes and greater complexity as they begin engaging with digital environments in new ways as teenagers.

5.1.3 Opportunity 3: Supporting Teachers' Knowledge and Practices through Flexible Conversation and Learning Tools. Though the environment in which we implemented our WYR scenarios with children was distinct from most formal classroom settings, we argue that this type of informal intergenerational dialogue and co-learning can also be leveraged in classroom learning contexts. Teachers expressed that some of the scenarios proved challenging and anxiety-inducing for them as adults, and that, in addition to considering how their students might respond to these dilemmas, they were inspired to think through how they might evaluate the pros and cons of various privacy and security decisions. Kumar and Byrne [31] note that teachers, who typically do not have formal training in privacy literacy, should not position themselves as authorities in related instructional interventions. While several of the co-facilitators in our sessions with children had significant expertise in privacy and security, we argue that such expertise is not required to engage in these types of discussions with children. By modeling their thought processes as they work through various personal concerns and priorities, educators can authentically communicate that privacy and security decisions are rarely clear-cut for children nor for adults. We envision that such an approach can support teachers and students in moving beyond the sorts of punitive rules and scare tactics characteristic of many traditional privacy and security learning approaches [29, 34, 38].

Our findings also suggest the utility and feasibility of our WYR approach in relation to teachers' busy work schedules and professional priorities. We argue that the usability (i.e., easy to learn, efficient to use, and replayable) and accessibility (inexpensive and technically easy to access and

modify) [64] of this privacy and security learning approach lies in its low-tech, simple, and flexible nature. The teachers in our study, many of whom were already using WYR activities with their students, commented on how easily they could modify the provided digital slide templates and scenario content in order to address arising needs and issues in their classrooms. Therefore, we propose that, in addition to being adaptable by researchers, designers, and developers, these tools must also be flexible and easily updated by teachers, who may vary in their teaching styles, content focus, and students populations.

5.1.4 Opportunity 4: Highlighting the Social and Emotional Aspects of Privacy and Security Learning. Finally, the most novel contribution of this study is arguably the insight it provides into the largely unexplored connections between privacy and security education and social and emotional learning (SEL). On the most basic level, teachers' eagerness to use hypothetical privacy and security dilemmas in their SEL curriculum suggests an opportunity to incorporate more and much-needed privacy and security education in elementary classrooms, particularly at a time when many schools are increasing their efforts to support students' mental health and SEL education [16]. Moreover, this avenue of research strikes us as particularly promising in light of children's prioritization of considerations related to their emotional safety (e.g., protecting themselves from embarrassment, asserting their agency and control over their private information) and social relationships (e.g., with parents, teachers, and friends) during our WYR discussions.

Additionally, in advocating for a SEL-based approach to privacy and security education, teachers in our study highlighted both the feasibilty of such an approach (i.e., that it would fit into their current SEL curriculum) as well as the importance of a holistic and comprehensive approach toward privacy and security education—one which can promote deeper learning (beyond a single self-contained activity or discussion) and help students draw connections between their emotions and their online experiences both within and beyond school. Moreover, our discussions with teachers alerted us to the potentially sensitive nature of facilitating privacy and security discussions with children who, unlike many of the children in our sample, may have less experience thinking and talking about technology in this manner. Indeed, prior research similarly demonstrates how privacy and security Choose-Your-Own-Adventure narratives developed by children often included drastic outcomes, such as murder and burglary, in response to routine missteps like sharing a password [30]. These findings further speak to the importance of accounting for and addressing children's possible anxiety associated with privacy and security topics. Thus, the proposal to frame privacy and security learning as a part of children's SEL learning strikes us as a unique opportunity to help children understand the sociotechnical nature of this domain—that is, how knowledge about the functional realities of surveillance and data collection are often tied to personal and social concerns, priorities and, in many instances, strong emotions [8, 27]. We believe that such an approach, as several teachers noted, can open new avenues for meaningfully connecting these concepts to children's current and future everyday lives.

5.2 Limitations and Future Work

Though we leveraged our collective privacy and security and childhood education expertise when developing and selecting our WYR scenarios, there are likely additional scenarios that were not captured at the time of the study. Future work can outline the links between specific privacy and security theories, such as contextual integrity [47], and additional privacy and security scenarios. Though we approach 'privacy and security' as intertwined and overlapping concepts in this work, many of our discussion prompts (e.g., 'What is one thing in your life that you want to keep private?', 'In all of these WYR challenges, your privacy is on the line. Have your thoughts changed about privacy? How?') and scenarios arguably foregrounded 'privacy' over 'security'. Thus, future work

should continue to expand relevant prompts by introducing more diverse concepts, including those that foreground security-related concerns. Additionally, future work could explore the characteristics of WYR privacy and security scenarios generated by teachers, parents, and children.

An additional limitation of this research is that the context in which we implemented our WYR scenarios (i.e., co-design groups characterized by deliberate efforts to minimize adult-child power dynamics and engender playful intergenerational collaboration) differed from most formal classroom settings. Each session was conducted remotely using Zoom and included no more than nine children, with adult-to-child ratios near one-to-one. The children who participated in each session also represented a variety of ages and grade levels, unlike most elementary classrooms. Though this offered valuable potential peer-to-peer learning support, it nevertheless made it difficult for us to disentangle certain developmental considerations and age-specific trends. These children were also perhaps more likely to have considered and discussed digital technology and related privacy and security topics than other children, due to their ongoing participation in co-design. Additionally, though we spoke with teachers across grades PreK-6, none of our child participants were in grades PreK-1, indicating a need for further research with with younger elementary-age children.

We recognize that this learning environment and level of adult support is uncommon in formal school environments and that open, equal, and informal communication between teachers and students is not necessarily the norm in all elementary classrooms. Additional research is therefore needed to understand how discussions centered around hypothetical privacy and security dilemmas play out among broader populations of children, in authentic elementary classroom settings, as implemented by teachers, and in comparison to other privacy and security classroom learning approaches. Such research will help determine the feasibility, learning outcomes, and additional contextual considerations of this and similar privacy and security learning approaches. Within this context, future work should also focus on identifying—not only how to scaffold these types of discussions for children—but also how to support teachers in open communication in those settings in which this atmosphere is not already a feature.

6 CONCLUSION

In this paper, we shared findings from our development of a technique for facilitating and expanding privacy and security discussions with elementary school children as a classroom learning activity. Based on our analysis of data from WYR sessions with children and interviews with elementary school teachers, we provide a set of recommendations for educators on how they might implement the activity in the classroom, and for how this technique can address the socio-emotional aspects of everyday privacy and security quandaries across a variety of contexts. We propose that WYR hypothetical dilemmas offer a simple yet powerful technique for promoting elementary aged children's engagement and agency with privacy and security concepts connected to their everyday lives. Given many children's and teachers' familiarity with the WYR game and the ease with which its scenarios can adapted, this learning approach can deeply engage learners in nuances and contextual factors that come into play in complex privacy and security situations which children may have encountered but have not yet had the opportunity to fully consider. Building on prior work [30, 32], we posit that it is critical for elementary learners to engage with privacy and security concepts in this manner in order to support them in making informed privacy and security decisions that align with their personal values and concerns now and in the future.

ACKNOWLEDGMENTS

We thank Amanda Lazar, Sunyup Park, and the anonymous reviewers for their valuable feedback on this paper, as well as all the children and teachers who shared their time and experiences with us. This project was funded by the National Science Foundation under awards 1951688 and 1951311.

REFERENCES

[1] Andria Agesilaou and Eleni A. Kyza. 2022. Whose data are they? Elementary school students' conceptualization of data ownership and privacy of personal digital data. *International Journal of Child-Computer Interaction* 33 (Sept. 2022), 100462. https://doi.org/10.1016/j.ijcci.2022.100462

[2] American Library Association. 2006. Information literacy standards for science and engineering/technology. https://www.ala.org/acrl/standards/infolitscitech

[3] Karla Badillo-Urquiola, Diva Smriti, Brenna McNally, Evan Golub, Elizabeth boyernsignore, and Pamela J. Wisniewski. 2019. Stranger Danger! Social Media App Features Co-designed with Children to Keep Them Safe Online *(IDC '19)*. Association for Computing Machinery, New York, NY, USA, 394–406. https://doi.org/10.1145/3311927.3323133

[4] Elana Blinder, Jessica Vitak, Marshini Chetty, Tamara L. Clegg, and Kevin Song. 2021. *Challenges and Opportunities Using Technology in the Classroom: Results From Focus Groups With Elementary School Teachers.* White paper. https://spe4k.umd.edu/wp-content/uploads/2022/02/SPE4K-Teacher-Focus-Group-Report-Anonymized-January-2022.pdf

[5] Jessi Boyer, Michael S Wendell, Jerry Alan Fails, Kendall House, and John Ziker. 2023. Evolutionary Perspectives on Novel Digital Environments: Parental Strategies in the Ecology of Fear. In *Proceedings of the 22nd Annual ACM Interaction Design and Children Conference* (Chicago, IL, USA) *(IDC '23)*. Association for Computing Machinery, New York, NY, USA, 688–692. https://doi.org/10.1145/3585088.3593878

[6] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. https://doi.org/10.1191/1478088706qp063oa

[7] Angela Calabrese Barton and Edna Tan. 2019. Designing for Rightful Presence in STEM: The Role of Making Present Practices. *Journal of the Learning Sciences* 28, 4-5 (Oct. 2019), 616–658. https://doi.org/10.1080/10508406.2019.1591411

[8] Tamara L. Clegg, Keaunna Cleveland, Erianne Weight, Daniel Greene, and Niklas Elmqvist. 2023. Data everyday as community-driven science: Athletes' critical data literacy practices in collegiate sports contexts. *Journal of Research in Science Teaching* 60, 8 (2023), 1786–1816. https://doi.org/10.1002/tea.21842

[9] Alma Leora Culén and Katie Coughlin. 2022. Growing Up in a Complex World: Engaging Children in Socio-Cultural Matters Through Speculative Installations. In *Designing Interactive Systems Conference*. ACM, Virtual Event Australia, 693–706. https://doi.org/10.1145/3532106.3533518

[10] Laurien Desimpelaere, Liselot Hudders, and Dieneke Van de Sompel. 2020. Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in Human Behavior* 110 (Sept. 2020), 106382. https://doi.org/10.1016/j.chb.2020.106382

[11] John Dewey. 1986. Experience and Education. *The Educational Forum* 50, 3 (Sept. 1986), 241–252. https://doi.org/10.1080/00131728609335764

[12] Dominic DiFranzo, Yoon Hyung Choi, Amanda Purington, Jessie G. Taft, Janis Whitlock, and Natalya N. Bazarova. 2019. Social Media TestDrive: Real-World Social Media Education for the Next Generation. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–11. https://doi.org/10.1145/3290605.3300533

[13] Stefania Druga and Rebecca Michelson. 2020. Research Toolkit for Family Speculative Play with Future Toys. In *Special Issue on Designing the future of technology with and for children*. INTERACT No 4, December 2020, University of Oulu, Finland. https://interact.oulu.fi/site/files/2020-12/interact-4-2020.pdf

[14] Allison Druin. 1999. Cooperative inquiry: developing new technologies for children with children. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems (CHI '99)*. Association for Computing Machinery, New York, NY, USA, 592–599. https://doi.org/10.1145/302979.303166

[15] Allison Druin. 2002. The role of children in the design of new technology. *Behaviour & Information Technology* (Jan. 2002). https://www.scinapse.io/papers/5048401

[16] Bree Dusseault. 2022. Building Upgrades, SEL: 100 Large & Urban Districts Plan Their Pandemic Recovery. https://www.the74million.org/article/building-upgrades-sel-100-large-urban-districts-plan-their-pandemic-recovery/

[17] Maurice J. Elias, Joseph Zins, and Roger P. Weissberg. 1997. *Promoting social and emotional learning: Guidelines for educators.* ASCD.

[18] Jerry Alan Fails, Mona Leigh Guha, and Allison Druin. 2013. Methods and Techniques for Involving Children in the Design of New Technology for Children. *Foundations and Trends in Human Computer Interaction* 6, 2 (Dec. 2013), 85–166. https://doi.org/10.1561/1100000018

[19] Paulo Freire. 2018. *Pedagogy of the oppressed.* Bloomsbury Publishing USA.

[20] Filippos Giannakas, Andreas Papasalouros, Georgios Kambourakis, and Stefanos Gritzalis. 2019. A comprehensive cybersecurity learning platform for elementary education. *Information Security Journal: A Global Perspective* 28, 3 (May 2019), 81–106. https://doi.org/10.1080/19393555.2019.1657527

[21] Mona Leigh Guha, Allison Druin, and Jerry Alan Fails. 2013. Cooperative Inquiry revisited: Reflections of the past and guidelines for the future of intergenerational co-design. *International Journal of Child-Computer Interaction* 1, 1 (Jan. 2013), 14–23. https://doi.org/10.1016/j.ijcci.2012.08.003

[22] Heidi Hartikainen, Netta Iivari, and Marianne Kinnula. 2016. Should We Design for Control, Trust or Involvement? A Discourses Survey about Children's Online Safety. In *Proceedings of the The 15th International Conference on Interaction Design and Children (IDC '16)*. Association for Computing Machinery, New York, NY, USA, 367–378. https://doi.org/10.1145/2930674.2930680

[23] Heidi Hartikainen, Netta Iivari, and Marianne Kinnula. 2019. Children's design recommendations for online safety education. *International Journal of Child-Computer Interaction* 22 (Dec. 2019), 100146. https://doi.org/10.1016/j.ijcci.2019.100146

[24] Mizuko Ito, Kris Gutiérrez, Sonia Livingstone, Bill Penuel, Jean Rhodes, Katie Salen, Juliet Schor, Julian Sefton-Green, and S Craig Watkins. 2013. *Connected learning: An agenda for research and design.* Digital Media and Learning Research Hub.

[25] Carrie James, Emily Weinstein, and Kelly Mendoza. 2019. Teaching digital citizens in today's world: Research and insights behind the Common Sense K–12 Digital Citizenship Curriculum. *Common Sense Media* (2019). https://pz.harvard.edu/resources/teaching-digital-citizens-in-todays-world

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

[27] Britney Johnson, Ben Rydal Shapiro, Betsy DiSalvo, Annabel Rothschild, and Carl DiSalvo. 2021. Exploring Approaches to Data Literacy Through a Critical Race Theory Perspective. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 706, 15 pages. https://doi.org/10.1145/3411764.3445141

[28] Stephanie M. Jones and Emily J. Doolittle. 2017. Social and Emotional Learning: Introducing the Issue. *The Future of Children* 27, 1 (2017), 3–11. https://www.jstor.org/stable/44219018

[29] 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 (Dec. 2017), 64:1–64:21. https://doi.org/10.1145/3134699

[30] Priya Kumar, Jessica Vitak, Marshini Chetty, Tamara L. Clegg, Jonathan Yang, Brenna McNally, and Elizabeth Bonsignore. 2018. Co-designing online privacy-related games and stories with children. In *Proceedings of the 17th ACM Conference on Interaction Design and Children (IDC '18)*. Association for Computing Machinery, New York, NY, USA, 67–79. https://doi.org/10.1145/3202185.3202735

[31] Priya C. Kumar and Virginia L. Byrne. 2022. The 5Ds of privacy literacy: a framework for privacy education. *Information and Learning Sciences* 123, 7/8 (Jan. 2022), 445–461. https://doi.org/10.1108/ILS-02-2022-0022

[32] Priya C. Kumar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2019. Privacy and Security Considerations For Digital Technology Use in Elementary Schools. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300537

[33] Priya C. Kumar, Fiona O'Connell, Lucy Li, Virginia L. Byrne, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2023. Understanding Research Related to Designing for Children's Privacy and Security: A Document Analysis. In *Proceedings of the 22nd Annual ACM Interaction Design and Children Conference (IDC '23)*. Association for Computing Machinery, New York, NY, USA, 335–354. https://doi.org/10.1145/3585088.3589375

[34] Priya C. Kumar, Mega Subramaniam, Jessica Vitak, Tamara L. Clegg, and Marshini Chetty. 2020. Strengthening Children's Privacy Literacy through Contextual Integrity. *Media and Communication* 8, 4 (Nov. 2020), 175–184. https://doi.org/10.17645/mac.v8i4.3236

[35] Maria Lamond, Karen Renaud, Lara Wood, and Suzanne Prior. 2022. SOK: Young Children's Cybersecurity Knowledge, Skills & Practice: A Systematic Literature Review. In *2022 European Symposium on Usable Security*. ACM, Karlsruhe Germany, 14–27. https://doi.org/10.1145/3549015.3554207

[36] Elmer Lastdrager, Inés Carvajal Gallardo, Pieter Hartel, and Marianne Junger. 2017. How effective is anti-phishing training for children?. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS '17)*. USENIX Association, USA, 229–239. https://dl.acm.org/doi/10.5555/3235924.3235943

[37] Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri. 2019. *Children's data and privacy online: Growing up in a digital age. An evidence review.* Monograph. London School of Economics and Political Science, London, UK. https://eprints.lse.ac.uk/101283/

[38] Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri. 2020. Data and Privacy Literacy. In *The Handbook of Media Education Research.* John Wiley & Sons, Ltd, 413–425. https://doi.org/10.1002/9781119166900.ch38

[39] Sana Maqsood. 2018. Evaluation of a Persuasive Digital Literacy Game for Children. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (CHI EA '18).* Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3170427.3180307

[40] Sana Maqsood and Sonia Chiasson. 2021. Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens. *ACM Transactions on Privacy and Security* 24, 4 (Sept. 2021), 28:1–28:37. https://doi.org/10.1145/3469821

[41] Sana Maqsood and Sonia Chiasson. 2021. "They think its totally fine to talk to somebody on the internet they don't know": Teachers' perceptions and mitigation strategies of tweens' online risks. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21).* Association for Computing Machinery, New York, NY, USA, 1–17. https://doi.org/10.1145/3411764.3445224

[42] Sana Maqsood, Christine Mekhail, and Sonia Chiasson. 2018. A day in the life of jos: a web-based game to increase children's digital literacy. In *Proceedings of the 17th ACM Conference on Interaction Design and Children (IDC '18).* Association for Computing Machinery, New York, NY, USA, 241–252. https://doi.org/10.1145/3202185.3202753

[43] Melissa Mazmanian and Simone Lanette. 2017. "Okay, One More Episode": An Ethnography of Parenting in the Digital Age. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17).* Association for Computing Machinery, New York, NY, USA, 2273–2286. https://doi.org/10.1145/2998181.2998218

[44] Brenna McNally, Priya Kumar, Chelsea Hordatt, Matthew Louis Mauriello, Shalmali Naik, Leyla Norooz, Alazandra Shorter, Evan Golub, and Allison Druin. 2018. Co-designing Mobile Online Safety Applications with Children. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18).* Association for Computing Machinery, New York, NY, USA, 1–9. https://doi.org/10.1145/3173574.3174097

[45] 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 (CHI '17).* Association for Computing Machinery, New York, NY, USA, 5197–5207. https://doi.org/10.1145/3025453.3025735

[46] Matthew B. Miles, A. Michael Huberman, and Johnny Saldana. 2018. *Qualitative Data Analysis: A Methods Sourcebook.* SAGE Publications.

[47] Helen Nissenbaum. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford University Press, Stanford.

[48] 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 (Oct. 2018), 5–32. https://doi.org/10.1515/popets-2018-0029

[49] Jenny Preece. 2004. Etiquette online: From nice to necessary. *Commun. ACM* 47, 4 (2004), 56–61.

[50] Farzana Quayyum, Daniela S. Cruzes, and Letizia Jaccheri. 2021. Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction* 30 (Dec. 2021), 100343. https://doi.org/10.1016/j.ijcci.2021.100343

[51] Victoria Rideout and Michael B Robb. 2017. *The Common Sense census: Media use by kids age zero to eight.* Technical Report. https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-kids-age-zero-to-eight-2020

[52] Lucy Simko, Britnie Chin, Sungmin Na, Harkiran Kaur Saluja, Tian Qi Zhu, Tadayoshi Kohno, Alexis Hiniker, Jason Yip, and Camille Cobb. 2021. Would You Rather: A Focus Group Method for Eliciting and Discussing Formative Design Insights with Children. In *Interaction Design and Children (IDC '21).* Association for Computing Machinery, New York, NY, USA, 131–146. https://doi.org/10.1145/3459990.3460708

[53] Mariya Stoilova, Sonia Livingstone, and Rishita Nandagiri. 2020. Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy. *Media and Communication* 8, 4 (Nov. 2020), 197–207. https://doi.org/10.17645/mac.v8i4.3407

[54] 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 *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21).* Association for Computing Machinery, New York, NY, USA, 1–34. https://doi.org/10.1145/3411764.3445333

[55] Kelly B. Wagman, Elana B. Blinder, Kevin Song, Antoine Vignon, Solomon Dworkin, Tamara Clegg, Jessica Vitak, and Marshini Chetty. 2023. "We picked community over privacy": Privacy and Security Concerns Emerging from Remote Learning Sociotechnical Infrastructure During COVID-19. *Proc. ACM Hum.-Comput. Interact.* 7, CSCW2, Article 245

(Oct 2023), 29 pages. https://doi.org/10.1145/3610036

[56] Ge Wang, Jun Zhao, Max Van Kleek, and Nigel Shadbolt. 2021. Protection or Punishment? Relating the Design Space of Parental Control Apps and Perceptions about Them to Support Parenting for Online Safety. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (Oct. 2021), 343:1–343:26. https://doi.org/10.1145/3476084

[57] Jon M. Wargo and Jasmine Alvarado. 2020. Making as worlding: young children composing change through speculative design. *Literacy* 54, 2 (May 2020), 13–21. https://doi.org/10.1111/lit.12209

[58] 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 (CSCW '15)*. Association for Computing Machinery, New York, NY, USA, 302–316. https://doi.org/10.1145/2675133.2675293

[59] Zheng Yan, Yukang Xue, and Yaosheng Lou. 2021. Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers. *Computers in Human Behavior* 121 (2021), 106791. https://doi.org/10.1016/j.chb.2021.106791

[60] Christine Ee Ling Yap and Jung-Joo Lee. 2020. 'Phone apps know a lot about you!': educating early adolescents about informational privacy through a phygital interactive book. In *Proceedings of the Interaction Design and Children Conference (IDC '20)*. Association for Computing Machinery, New York, NY, USA, 49–62. https://doi.org/10.1145/3392063.3394420

[61] 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*. ACM, Glasgow, Scotland, UK, 1–15. https://doi.org/10.1145/3290605.3300303

[62] Jason C. Yip, Kiley Sobel, Caroline Pitt, Kung Jin Lee, Sijin Chen, Kari Nasu, and Laura R. Pina. 2017. Examining Adult-Child Interactions in Intergenerational Participatory Design. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Association for Computing Machinery, New York, NY, USA, 5742–5754. https://doi.org/10.1145/3025453.3025787

[63] Leah Zhang-Kennedy, Yomna Abdelaziz, and Sonia Chiasson. 2017. Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. *International Journal of Child-Computer Interaction* 13 (July 2017), 10–18. https://doi.org/10.1016/j.ijcci.2017.05.001

[64] Leah Zhang-Kennedy and Sonia Chiasson. 2021. A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *Comput. Surveys* 54, 1 (Jan. 2021), 12:1–12:39. https://doi.org/10.1145/3427920

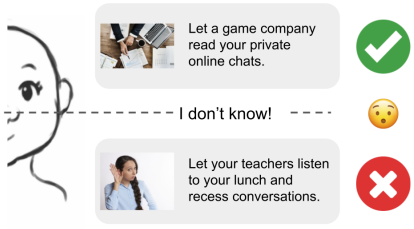
[65] Leah Zhang-Kennedy, Christine Mekhail, Yomna Abdelaziz, and Sonia Chiasson. 2016. From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats. In *Proceedings of the The 15th International Conference on Interaction Design and Children (IDC '16)*. Association for Computing Machinery, New York, NY, USA, 388–399. https://doi.org/10.1145/2930674.2930716

[66] Jun Zhao, Blanche Duron, and Ge Wang. 2022. KOALA Hero: Inform Children of Privacy Risks of Mobile Apps. In *Proceedings of the 21st Annual ACM Interaction Design and Children Conference (IDC '22)*. Association for Computing Machinery, New York, NY, USA, 523–528. https://doi.org/10.1145/3501712.3535278

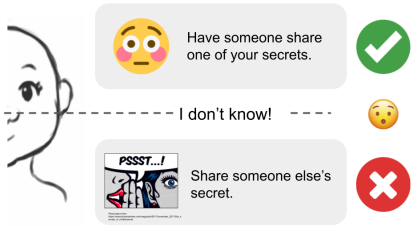
[67] Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. 2019. 'I make up a silly name': Understanding Children's Perception of Privacy Risks Online. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland, UK) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300336

A APPENDIX

A.1 Additional Would You Rather Prompts Used in Focus Groups With Children



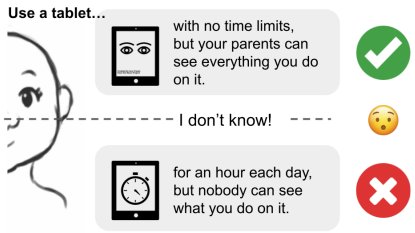
(a) WYR#2: Information Sharing:Corporations/Companies



(b) WYR#4: Information Sharing: Personal Data

Fig. 2. Would You Rather Prompt Slides for Information Sharing scenarios used in the remote sessions

(a) WYR#5: Advertising/Tracking:Social Media



(b) WYR#6: Advertising/Tracking:Online Activities

Fig. 3. Would You Rather Prompt Slides for Advertising/Tracking scenarios used in the remote sessions

A.2 Teacher Focus Group Protocol/Interview Guide

Moderator: Welcome and thanks for joining us for this focus group. [Moderator introduces herself and other researchers, if present]. We're researchers from [the University of Maryland/University of Chicago]. We've partnered with two elementary schools to develop curricula that helps students learn how to navigate technology, with a focus on digital privacy and security. We're creating "micro-lessons," which are short activities that introduce a topic around online privacy and security and can be inserted into your normal curricula. Rather than just developing materials on our own and asking you to test them in your classrooms, we want to leverage your expertise to ensure that the materials we create will be practical and meaningful for your classrooms. Today's conversation is part of the second phase of the project, where we want to co-design micro-lessons with you. In the future, we want to work with you to evaluate the micro-lessons with your students.

Over the next [40 / 60] minutes, we're going to first share an example of an activity we've been testing with kids ages 7-13. We'd like to get your initial reactions to this activity. After we go through the example, we will have a set of questions we'd like to open up to discussion about how you might add on to or adapt this activity for the children you teach. Think of this more as a conversation than a formal interview, and we encourage everyone to share their thoughts. Our

role is merely to facilitate the conversation; you all will be guiding it.

Before we get started, I'm going to start recording. This conversation will remain confidential, and any quotes we use will be attributed to pseudonyms. Does anyone have questions before we start?

Ice-Breaker, WYR Overview, General Feedback
Moderator: Great. Let's start with a quick warm-up activity. Could we have each person share their name and what grades and subjects they teach?

Moderator: Now let's talk about one of the games we've been working on that could be part of a micro lesson activity in the classroom. Maybe you've heard of the game, Would You Rather, where you have two options and you have to pick one. For example, someone might ask, "Would you rather only eat pizza or ice cream for the rest of your life?" Then people pick a side, maybe move to either side of the room, and they can explain their choice. We thought this would be a useful way to have conversations about privacy and security with kids in a classroom setting, so we tested this out with three different groups of children. Note that we did this over Zoom but it would probably be easier in person, where students could get up and move around the classroom. Let me show you a couple examples we used in our sessions. [Show slides.]

Imagine you're going to use this in your classroom. We need your expertise on how to introduce this activity and what it would look like for you to be able to successfully integrate it into class.

Does anyone have thoughts about the content and structure of an activity like this and whether you think this would prompt student engagement and discussion?

Breakout Sessions
NOTE: Depending on size of the group/amount of conversation, the next part can happen as a group or in breakouts. If using breakouts, try to have a research team member in each room to start recording. Organize rooms by grade band, if possible.

Moderator: We're going to put you into breakout groups to discuss how you could adapt and/or extend this activity for your students. Think about the structure and content around the activity, including how you might introduce the activity and challenges you might face in getting your students to engage. Also think about ways you could extend the lesson beyond the classroom, such as through a take-home activity kids could do with a family member. Make sure to choose one person in your room who will report back at the end.

[Notes: Walk through slide deck. Explain that they can use their slide to take notes, add a second slide if needed. If there aren't breakouts, one of the team members can take notes as people talk. Create a separate slide for each aspect (ideas on adapting/changing structure; challenges; extending activity; new WYR questions; additional resources).]

Breakout Discussion Questions

- How this activity might need to change based on the grade / age of students
- Ideas for how you would change the structure of this activity
- Ideas for how to extend this activity (including what a take-home activity looks like)
- Additional ideas for WYR questions

- The format/content of supporting documents to help you run this in class and/or supporting materials for parents

Moderator: Report back from breakouts in 1-2 minutes. [wait for reports] Great. To wrap up, is there anything else you'd like to share that might be relevant for the project? Do you have any questions for us?

Closing Remarks
Before we go, we're planning to run additional sessions in coming months to go through other activities we've been working on. We could do them in short bursts like this, or in a longer session like a workshop.

- If we do any more sessions during the school year, is this the best time?
- Are there other staff we should be contacting directly to encourage them to participate?

We'll also be in touch later this year to recruit 3-4 teachers across the different grades to work more closely with us next school year and to do pilot runs of the activities.

[Thank participants and let them know the gift card is on the way.]

A.3 Full Codebooks for WYR Session And Interview Analyses

Received July 2023; revised October 2023; accepted November 2023

Code Name	Description
Privacy and Security Concerns And Non-concerns	**Children express concern/investment (or lack of) in one/more privacy and security aspects of a WYR scenario.**
*Subcode: embarrassment	Children express concerns/non-concerns related to prospect of personal embarrassment.
*Subcode: nothing-to-hide	Children express a lack of concern related to the hypothetical surveillance and consumption of their personal information by others.
*Subcode: personal relationships	Children reference personal relationships (e.g., with parents, with friends) as a factor in concern regarding hypothetical privacy and security infractions.
*Subcode: surveillance	Children express concerns/non-concerns related to different forms of surveillance.
*Subcode: trust	Children reference how level of trust (in individuals, commercial organizations, etc.) influences their concern regarding hypothetical privacy and security infractions.
Elaboration: Real-Life Connections	**Children connect a WYR scenario to first-hand or second-hand (family members,' friends', fictional characters', etc.) real-life experiences.**
*Subcode: family and peer relationships	Children reference the influence of family members' and/or peers' privacy and security experiences in explaining rationale for a WYR decision.
*Subcode: family and school norms	Children reference the influence of their status quo home and/or school rules, privileges, and norms as a factor in a WYR decision.
*Subcode: social media, games and internet use	Children reference experiences related to their use and/or prior knowledge of social media, online games, and other forms of internet use.
*Subcode: texting and chatting behaviors	Children reference experiences related to their use and/or prior knowledge of different forms of online texting and chatting.
Elaboration: Considering Tradeoffs	**Children elaborate upon the perceived pros, cons, and tradeoffs influencing their WYR decisions.**
*Subcode: pros and cons	Children explicitly discuss some of the pros and cons associated with one or more aspects of a WYR scenario.
*Subcode: loopholes and extreme cases	Children propose workarounds (loopholes) or an imaginative/unexpected example situations (extreme cases) influencing their WYR decisions.
Facilitator Moves	**Adult participants add questions, comments, or other actions to elicit additional thinking and elaboration from child participants.**
*Subcode: modeling thought process	Adult participants demonstrate the thought process informing their WYR decisions.
*Subcode: summarizing/elaborating children's responses	Adult participants paraphrase contributions of children and/or express how what's been said connects to other aspects of the discussion.
*Subcode: changing scenario criteria	Adult participants revise the original scenario criteria during post-voting discussion.
*Subcode: posing questions	Adult participants pose follow-up questions to children after post-voting discussion.

Table 5. Codebook for WYR Session Analysis

Code Name	Description
Classroom Implementation Context	Teacher describes details about their school/classroom context, their existing instructional approaches, and/or their students' characteristics
When/Where	Teacher describes when and how this activity might fit into their day/curriculum.
Instructional Approach	Teacher describes how the activity would be implemented (e.g., whole class, small group, individual, homework, etc.)
Activity Function	Teacher describes what function the activity would serve (e.g., warm-up, main lesson activity, assessment, etc.)
Liked	Teacher mentions something they like about the activity.
Concerns and Additional Considerations	Teacher discusses something that might not work or that should be considered in relation to their or other students/classrooms/school settings.
Suggested Modifications	Teacher makes a recommendation for improving existing activity to better meet their students'/classrooms' needs.
Proposed Extensions	Teacher recommends an extension to the existing activity (e.g., an additional writing prompt, illustrated activities, etc.)
Home-School Connection	Teacher recommends ideas for connecting in-class learning to home-based learning and/or about educating or collaborating with families.

Table 6. Codebook for Teacher Interviews Analysis