Towards Understanding Family Privacy and Security Literacy Conversations at Home: Design Implications for Privacy Literacy Interfaces

Kenan Kamel A Alghythee
kalghy2@uic.edu
University of Illinois Chicago
Chicago, IL, USA

Adel Hrncic
ahrnc2@uic.edu
University of Illinois Chicago
Chicago, IL, USA

Karthik Singh
ksingh49@uic.edu
University of Illinois Chicago
Chicago, IL, USA

Sumanth Kunisetty
manikrk1@umbc.edu
Univ. of Maryland Baltimore County
Baltimore, Maryland, USA

Yaxing Yao
yaxing@vt.edu
Virginia Tech
Blacksburg, Virginia, USA

Nikita Soni
nnsoni@uic.edu
University of Illinois Chicago
Chicago, IL, USA

ABSTRACT

Policymakers and researchers have emphasized the crucial role of parent-child conversations in shaping children's digital privacy and security literacy. Despite this emphasis, little is known about the current nature of these parent-child conversations, including their content, structure, and children's engagement during these conversations. This paper presents the findings of an interview study involving 13 parents of children ages under 13 reflecting on their privacy literacy practices at home. Through qualitative thematic analysis, we identify five categories of parent-child privacy and security conversations and examine parents' perceptions of their children's engagement during these discussions. Our findings show that although parents used different conversation approaches, rule-based conversations were one of the most common approaches taken by our participants, with example-based conversations perceived to be effective by parents. We propose important design implications for developing effective privacy educational technologies for families to support parent-child conversations.

CCS CONCEPTS

• **Human-centered computing → Empirical studies in HCI**.

KEYWORDS

Family, Privacy, Security, Literacy, Parents, Children, Education Technology

ACM Reference Format:
Kenan Kamel A Alghythee, Adel Hrncic, Karthik Singh, Sumanth Kunisetty, Yaxing Yao, and Nikita Soni. 2024. Towards Understanding Family Privacy and Security Literacy Conversations at Home: Design Implications for Privacy Literacy Interfaces. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3613904.3641962

CHI '24, May 11–16, 2024, Honolulu, HI, USA

ACM ISBN 979-8-4007-0330-0/24/05
https://doi.org/10.1145/3613904.3641962

1 INTRODUCTION

Children are using technology more frequently and at younger ages [27]. In 2013, 75% of children under nine used a tablet or smartphone at home [26], and these usage patterns have been increasing since. Despite age restrictions, 12% of 9-year-olds used one or more social media sites, increasing to 34% by age 11 [22]. With the rise of cyberbullying, online predators, and hacking of smart home devices, it is important for children to develop online privacy and security literacy [21, 29]. Privacy literacy is not just about knowing facts, but about having critical thinking and decision-making skills to interpret digital scenarios and act in ways that respect privacy [14, 15]. In this paper, we define privacy literacy as *"the practice of enacting appropriate information flows within sociotechnical systems"* [14, 15]. This means children must understand and analyze different digital contexts, assess what is suitable behavior in that context, comprehend the implications of information sharing, and decide on appropriate actions. [14, 15]. While children of all ages have some basic terminology understanding of online privacy and security [31], this is not enough to foster the development of privacy and security decision-making skills. [14, 15]. The ability to make informed decisions is particularly critical for preteens, as they transition from parental supervision to greater online independence [14]. For this study, we acknowledge that both "online privacy" and "online security" are broad, complex terms for which descriptions depend on audience and context [31]. Since there is no common definition for them [10], we use a comprehensive perspective that includes privacy and security literacy within cybersecurity literacy.

Parent-child conversations are one of the most effective ways to influence children's privacy and security decision-making skills [18, 31]. As such, policymakers and researchers have emphasized the need for creating education technologies and materials that enable effective parent-child conversations about digital privacy and security [17, 34]. However, despite this emphasis, little is known about what existing parent-child conversations look like, including their context, characteristics, and level of children's engagement during conversations. To enable us to design better privacy literacy technologies for families that are tailored to their needs and

preferences, it is important to have an understanding of existing practices. Online privacy and security concepts are abstract, making it difficult for children to understand and apply in real-world [32], especially for children under 13, who are still developing their abstract thinking abilities [15, 31, 32]. Parents also face challenges in communicating privacy and security concepts to children, due to its abstract nature [15, 31], and often have misconceptions about the relevance of discussing privacy with young children [14]. The challenges faced by both children in understanding and parents in communicating these concepts could significantly influence the nature of parent-child conversations. One of the closely related prior works by Williams et al. [31] explored the influence of parents on children's understanding of cybersecurity literacy and noted the importance of parent-child conversations. However, this work did not delve deeply into understanding the nature of the parent-child conversation and called for further research to *"qualitatively explore the types of privacy-related conversations that parents engage in with their children, which could help develop a better understanding of exemplary characteristics of such discussions."* Our research takes a first step towards answering this call. By gaining insights into existing conversation practices, we can design effective privacy and security literacy technologies for families that more intentionally support and augment existing ways of parent-child discussions at home. To address this gap and answer our research questions, we interviewed 13 parents of children ages 13 and under:

- **RQ1**: What types of conversation approaches do parents employ during privacy and security literacy discussions with their children at home?
- **RQ2**: To what extent are children engaged in these parent-child conversations?
- **RQ3**: How can we take existing parent-child conversation approaches into account when designing privacy and security literacy interfaces tailored for families?

Parents in our interview study reflected on their existing privacy literacy practices and conversational strategies at home. We qualitatively analyzed the interview data using inductive thematic analysis to identify parent-child conversation approaches, parents' perceptions of children's engagement during these conversations, and parents' suggestions to inform the design of future privacy literacy technologies for families. Our analysis led us to contribute a novel and systematic categorization of five distinct parent-child privacy and security conversation categories: rule-based, example-based, exposing decision-making, consequence-based, and contextual conversations (**RQ1**). For example, rule-based conversations involve parents establishing do's and don'ts for children's online actions, while example-based conversations involve showing real-life tangible examples such as phishing emails, and context-based conversations include parents discussing privacy actions and decision-making about a specific application context. Overall, we found that parents often employed a combination of these conversational approaches, with rule-based conversations being one of the most common methods. Our findings showed the potential of example-based conversations as being effective in helping children develop privacy literacy skills. Parents in our study discussed that although young children (aged 10 and under) engaged in these conversations (**RQ2**), their understanding of digital privacy and security was often simplistic and not as nuanced as needed to make decisions online. Parents also discussed facing challenges in conveying the nuances of privacy decision-making processes to children. For example, difficulty in articulating the appropriateness of privacy actions based on the application context, such as sharing location on maps compared to refraining from doing so on Snapchat. We propose important design implications for developing effective privacy educational technologies for families that support parent-child conversations (**RQ3**). In doing so, our research contributes to SIGCHI and cybersecurity education communities. Our findings examine and systematically characterize five categories of privacy and security conversations among families. Nevertheless, our study encourages the research community to explore which of these categories are the most effective in helping support children's privacy and security literacy and to think critically about how to afford them in more meaningful ways in a family setting through educational technology. We make the following unique research contributions:

- We developed a characterization of five types of parent-child conversation methods presented in Table 2, based on empirical insights from our interview study. This categorization can serve as a starting point for researchers and designers of privacy literacy education technology to create interfaces that facilitate family discussions to enhance children's privacy and security decision-making skills.
- Our findings shed light on parents' perceptions of their children's engagement during privacy and security conversations and suggestions on how to design collaborative educational interfaces effectively to better support children's privacy and security literacy experiences at home. The existing literature lacks substantial insights on designing collaborative privacy and security literacy interfaces for families.
- We propose important design implications for creating future privacy literacy interfaces that leverage families' existing conversation practices and more directly afford engaging experiences for children.

The findings of this work will forge pathways to design effective privacy literacy technologies tailored for families.

2 RELATED WORK

We situate our study within two research areas: (1) the significance of parent-child conversations for privacy literacy and (2) privacy literacy interfaces for children.

2.1 Significance of Parent-Child Conversations for Privacy Literacy

Multiple prior works have highlighted the importance of discussion between parents and teens [1, 2, 11] to support teen's online privacy and safety. For instance, Ghosh et al. [11] designed and evaluated the Circle of Trust Android application with 17 parent-teen pairs, aimed at promoting trust and active conversation between families. In their findings, the authors found that parents preferred this app as it engaged teens in the oversight process over merely relying on parental control tools. Although this prior work was in the context of teens, it lays the groundwork for a shift from solely relying on parental controls towards promoting family-centric privacy and security discussions. Such family discussions are more important

for preteens who are still learning to think abstractly and shifting towards making more independent online privacy-related decisions. Children view privacy as the ability to control their personal information and prevent unwanted individuals from accessing it [5]. However, their concerns differ from those of adults, as preteens prioritize safeguarding their immediate social networks from sharing embarrassing information about them online, while adults prioritize protecting children from malicious strangers who may use their personal information [6]. This underscores the divergence in the approaches to digital life between adults and children.

Research has indicated that children acquire their beliefs about privacy from their families and develop critical thinking skills for privacy decision-making through conversations [5]. However, not all parent-child conversations inherently lead to the development of effective privacy-related critical thinking skills. It is crucial to intentionally scaffold these conversations to incorporate discussions about the critical dimensions of digital privacy that children need to consider when making privacy-related decisions. Designing educational interfaces to scaffold these conversations requires a better understanding of the existing state of parent-child privacy conversations [14]. As an example, Hashish et al. [12] investigated how to design a content filtering prototype that lets parents and children (ages 6-8) work together while also providing discussion opportunities. The prototype supported parent-child mode where they created filters collaboratively, supporting the need for involving parents and children together in content filtering decisions. Based on their findings, Hashish et al. [12] called for more work on the nature of parent-child dialogues that could more effectively foster children's privacy decision-making skills. Along this line, Williams et al. [31] conducted a study with parents and elementary and middle school children to understand how parents influence children's privacy and security understanding. Their findings hinted at conversations families have, including consequence-based conversations where parents discuss the consequences of certain privacy actions with children. However, the paper did not go deep into exploring the conversation approaches used by parents. Based on their analysis, Williams et al. [31] called for deeper qualitative explorations into the kinds of conversations that parents have with children. We take a step towards addressing this gap in our paper.

Our key goal is to gain an in-depth understanding of how parents and children ages under 13 talk about privacy and security. As the first step, we initially focus on parents as our participants because young children, in their critical phase of cognitive development, may not remember or convey the full range of conversations they have had with their parents. Parents are often the very first source of information for young children, and this is especially true in the context of privacy, where children learn behaviors and norms by observing and interacting with adults [5]. Uncovering parents' perspectives can provide a necessary foundation for later incorporating children's perspectives and assessing the effectiveness of different conversational approaches. Our study goes beyond prior work by systematically categorizing five types of parent-child privacy and security conversational approaches and by analyzing parents' perceptions of children's engagement during these discussions, which have not been explored in the literature yet.

2.2 Privacy Literacy Interfaces for Children

While not targeting family groups as their primary audience, several prior works have developed privacy literacy technologies to support cybersecurity education and awareness among children [23, 34], including e-books, computer games, and multi-touch tabletop interfaces. Leveraging the zone of proximal development and scaffolding children's privacy strategies was shown to be a useful approach to teach children how to protect themselves online [16, 35]. Prior work has demonstrated the effectiveness of games and interactive stories in educating children about privacy [16]. Analogies and metaphors used to present abstract complex topics into understandable items and behaviors also help children understand privacy concepts [25]. Raynes-Goldie and Allen [24] created a digital tabletop game called "*The Watchers*," aiming to teach children about online privacy issues and inform their decision-making regarding sharing personal information online. Although the effectiveness of the digital tabletop game was not evaluated, their preliminary observations highlighted the importance of involving children as design partners and supporting interactive discussion-based cybersecurity learning. Another example is Cyberheroes [33], a narrative educational e-book for children ages 7-9. When reading the e-book, children follow privacy superheroes as they navigate situations involving cyberbullying, location tracking, and password security.

In a 2020 survey Zhang-Kennedy and Chiasson [34] reviewed multimedia interfaces developed between 2000-2019 for cybersecurity awareness and education, including digital games, films, and digital tabletop interfaces. They found that out of 119 tools, 51 targeted children or youth, but none explicitly targeted families as a learning unit. With the growing recognition of privacy literacy as a family learning component (e.g. by MediaSmarts [17] and Common Sense Education [8]) there is a need to explore how multimedia educational tools can be designed to support family group learning. Our study fills this gap, by serving as a step toward understanding the nature of privacy-related parent-child conversations and leveraging this understanding to discuss implications for designing privacy literacy technology for families.

3 METHODOLOGY

In this section, we describe our study methodology.

3.1 Participants

Since parents are often the very first source of privacy and security-related information for children [5], uncovering their perspectives on the range of parent-child conversations can provide a necessary foundation for later incorporating children's perspectives. We interviewed 13 parents or guardians of at least one child ages 13 or under. Participants aged between 35 to 64 (9 F, 4 M). All of our participants reported having at least a Master's degree. 5 participants had 2 children, 5 had 3 children, 2 had one child, and 1 participant had 4 children. 12 of our participants had at least one child ages 10-13, and 3 participants had at least one child ages 5-9, and 2 participants had at least one child ages 5 and under (Table 1). During the interview and the demographic form-filling process, discrepancies were observed in the reported age groups of the children by two participants. We decided to use the age group information

Table 1: Demographics of participants in our study. The Frequency row lists participant responses to how frequently they discuss privacy and security concepts with children (QO: Quite often, O: Often, MFT: More than a few times).

ID	P463	P880	P313	P669	P247	P324	P990	P724	P765	P905	P523	P810	P753
Kids' age	10-13, 13+	10-13	10-13, 13+	10-13, 13+	10-13, 13+	1-2, 5-7, 8-9	10-13, 13+	8-10, 10-13	10-13	3-4, 8-9, 10-13	10-13, 13+	10-13, 13+	10-13, 13+
# of Kids	3	1	2	2	4	3	2	2	1	3	3	2	3
Frequency	QO	MFT	QO	MFT	QO	O	O	O	QO	O	O	QO	QO

provided during the interview. The majority of our participants (8) mentioned they discussed privacy and security topics with their children quite often or more than a few times (Table 1), with all participants mentioning "home" as the place where these discussions took place. All of our participants mentioned that their kids regularly use technologies such as smartphones, tablets, or smart home devices. Our paper aims to understand how parents discuss privacy topics with their children ages 13 and under. We did not include data from one participant who had kids ages over 13 in our reported analysis. We defer the comparison of parents' conversational approaches for teenagers (ages 13+) versus younger children to future work.

3.2 Procedure

The participants were recruited by sending a study recruitment advertisement to a general university employee email listserv. Each participant filled out an interest form that asked about their children's grade level. Then we conducted online semi-structured interviews [3] with the participants. All participants were sent a digital consent form to read and sign before the start of the online study. All interviews were conducted via university Zoom and were video recorded. All interviews followed the discussion guide created by the research team (Appendix A). The duration of interviews ranged from 20 to 59 minutes. The interview questions were structured around parents' approaches to discussing digital privacy topics with children, their impressions of children's engagement with the content, sources of privacy knowledge, and parents' perception of how well their current approach to privacy literacy is working. After answering interview questions, participants participated in a design probe activity [13] where participants were shown an existing privacy literacy web page by Common Sense Media [7], and they were prompted to discuss how they might teach the listed concepts to children (see supplemental materials for web page screenshot and design probe questions). The study was approved by the university's institutional review board. All participants received a $15 gift card for participating in the study.

3.3 Data Analysis

To uncover conversation methods employed by parents when discussing privacy topics with children, our research team transcribed the interview data and analyzed transcripts using inductive thematic analysis, based on Braun and Clarke's approach [4]. Inductive thematic analysis is a bottom-up approach used to systematically organize large-scale qualitative data into themes based on their natural relationships, without fitting the data into a pre-existing coding scheme [4]. The analysis involved six phases: familiarizing yourself with the data, generating preliminary codes based on the data, searching for themes, reviewing themes, defining and naming themes, and finally presenting themes [4]. To start the analysis, three researchers individually read the transcripts to become familiar with the data and grouped participant quotes based on preliminary codes (see supplemental materials for preliminary codes): one researcher read and grouped 100% of the transcripts, and two other researchers read 57% and 43% each. Next, three researchers came together as a group over several meetings to review all the interview data based on preliminary codes and capture the emergent themes across different codes related to parent-child conversations. During our discussion meetings and iterations, some conversation themes collapsed into each other and some were broken into independent themes. In the end, we came up with the following themes: parents' role, parents' motivation, types of parent-child conversations, parents' perception of children's engagement, and implications for privacy literacy technology design.

4 FINDINGS

The main goal of this paper is to understand what conversational approaches parents employ when discussing privacy and security topics with children, and parents' perceptions of how children engage in these conversations. We present our analysis divided into (1) **role of family conversations** for privacy and security literacy, (2) what **motivates** parents to have privacy and security-related conversations with children at home, (3) what is the **nature** of parent-child conversations, (4) parents' perception of which type of conversations **engaged** children, and (5) how do parents think of **explaining abstract privacy concepts** to children.

4.1 What is the Role of Family Conversations for Privacy and Security Literacy?

During our analysis, we observed that parents frequently mentioned family conversations as an overarching theme for the education and guidance of their children regarding digital privacy and security decision-making skills. Some parents found that repeatedly verbalizing the rules and guidelines was an effective strategy for instructing their children about online privacy and safety. For instance, one parent emphasized this approach, stating, "*Besides verbally telling them, I think it worked. I haven't seen them in any website that raise questions or raise concerns, so, besides verbally tell them ... it's really, what, it's the best you can do, you have to be verbally enforced it to them ...*" [P724]. Parents predominantly perceived themselves as

conversation initiators and educators, as exemplified by the statement, "*... we, our main method of controlling all of it is conversations and an openness, trying to mmm, they do know that their phones are also our phones, so, we reserve the right at any point to look at them.*" [P463]. Parents also acknowledged the necessity of employing monitoring devices to reinforce these instructions, if needed, "*..... you have to be verbally enforced it to them, and you can go as far as putting monitoring devices but I don't want to ...*" [P724] and "*Look at my daughter's phone, I do have software on her phone, which she has figured out how to take of which I put back on but that does track what ... she's looking, at.*" [P669]. Parents of younger children often expressed a desire to gradually guide their children into the digital world while grappling with uncertainty regarding the appropriate age to initiate this process. As one parent articulated, "*We want her to slowly have, like, we want to do a slow release of responsibility with her so that it's not she doesn't go crazy when she gets it. We want to kind of guide her through that, but we're not really sure what the appropriate age is to start that is.*" [P905]. **In general, we saw parents emphasizing the significance of family discussions as a means to educate both younger (ages <10) and older (ages 10-13) children about digital privacy and security.**

4.2 What Motivates Parents to have Privacy and Security Conversations with Children at Home?

We analyzed the parents' motivations to initiate privacy and security conversations with children, and uncovered diverse factors that prompted the discussions. We saw parents taking their child's developmental needs and real-world incidents that children encountered online as a catalyst for driving such family discussions. For example, one parent highlighted the importance of discussing privacy and digital identities during children's formative years when they may not fully grasp the nuances of online interactions: "*I think the kids' identities need to be protected while they are in these ages and stages where they don't understand the nuance so ...*" [P463]. Significant lifestyle changes and milestones in their children's lives also encouraged parents to engage in these digital privacy conversations. For example, the same parent said: "*... each [child] has a debit card that's linked online and all of that, that was kinda our first conversation around protecting your identity ...*" [P463]. Another parent shared anecdotal instances of their child receiving unwelcome invitations and online bullying, which prompted discussions surrounding online safety: "*And she's getting, you know, invites from men that are in their thirties and forties... do you see why I want you to have a private account because these individuals would have data on you and would be able to see what you're doing, where you are, who your friends are.*" [P990] and " *... and my children have had some really nasty comments posted towards them. So, I have seen the immediate drawbacks.*" [P990]. We also saw parents using incidents they came across through the news as an opportunity to start discussions with children: "*I am yeah I mean whenever there's something online or something in the news is an opportunity to bring it up ... atleast on a monthly basis.*" [P313]. **Overall, we saw real-world incidents, life changes, and parents' care for children's future due to digital consequences as a motivating component to drive parent-child privacy conversations**.

4.3 What is the Nature of Parent-Child Conversations?

The goal of our analysis was to uncover the nature of conversation approaches parents use to engage children in discussion regarding privacy and security concepts, and not to definitively identify the most effective parent-child conversation approach. As shown in Table 2, we identified five distinct types of parent-child conversation categories: (1) rule-based, (2) example-based, (3) expose decision-making processes, (4) consequence-based, and (5) contextual conversations. We also found that parents often used a combination of these conversational approaches when communicating with their children. These findings regarding the conversation categories employed by parents will serve as a foundation for guiding further research into understanding which approaches might be most effective for children's privacy literacy. Next, we will provide an in-depth explanation of each conversation category.

4.3.1 ***Rule-based Conversations.*** During our analysis, we saw a recurrent theme of parents asking children to adhere to specific rules and regulations regarding what they should do and not do while online, such as instructing not to share passwords, personal data, and location information with others. One parent in our study expressed their stress about children's privacy and online actions and had them sign contracts about rules: "*I hate it, it's a very stressful part of parenting for this generation of those of us kinda , kinda figuring out as we go, mmm, I have had them sign contracts before they're allowed to text, know these sorts of things.*" [P463]. Other parents similarly mentioned employing rule-based discussion approaches to tell their child not to share data or post anything online: "*For my second son, I always tell him, hey, don't just share you data online cause you don't know who is out there, so yes, we do talk about it almost on a weekly basis.*" [P724] and "*We should not to share we should not to post your online something like that.*" [P880]. In addition, we saw parents telling their children not to upload vacation photos with geolocation tags: "*When you go on vacation, don't post pictures that we're, "here we are in California".*" [P990]. While discussing these rules with children, a central point was parents highlighting that anything posted online is irreversible and cannot be removed: "*[I] have been pretty repetitive and saying that anything you post is permanent. It can be taken out of context.*" [P990]. Parents also set forth explicit guidelines for their children to adhere to when engaging with unfamiliar individuals online: *"I keep re-iterating myself and what it means to not share personal information... don't tell them what time you're at home you don't tell them what time you're leaving you don't give information of you ..."* [P753]. When communicating these rules, parents *hoped* that children would apply and translate these rules discussed in a general context to diverse online contexts and scenarios: "*Yeah, I don't know if they're on Snapchat but yeah, I try to tell them I tell them to disable it [location] ...I haven't like look in their phone ..., I tell them and hope that they are listening.*" [P313].

4.3.2 ***Example-Based Conversations.*** The example-based conversation is another approach employed by parents to discuss privacy-related topics with children. In this approach, parents mentioned about "showing" tangible examples during conversations to contextualize what they were talking about rather than just "telling", and have found it effective: "*I actually think, you know,*

Table 2: Categories of Parent-Child Privacy and Security Conversations.

Conversation Category	Definition	Examples from Transcripts
Rule-based Conversations	Parents tell children about rules (do's and don'ts) they should follow regarding digital privacy and security	*"... before you start this game this is what we do, this is the ground rules, you may not talk to anybody online," you know, "that you don't know, you may not share this specific information ...."*
Example-based Conversations	Parents use tangible examples (e.g., phishing emails) to discuss privacy and security concepts with children	*"...I so I kinda showed them that email so they can see kinda how, it was Paypal, that what it was, it was like a fake Paypal one, and how it looks like ... "*
Decision-making Process Conversation	Parents expose their own decision making thought process behind privacy actions, in other words, what rationale guide their digital privacy actions or recommendations	*" ... so I'm trying to show them what I do ... I was like, "where did you get this site from?" You know, "was it from the actual site or was it you know, a link that was sent to you", so I'll ask those questions before I enter... my...credit card information"*
Consequence-based Conversations	Parents highlight the consequences of privacy actions to children in order to make children aware of what might happen if caution is not taken	*"...I tell him hey if you don't create a strong password, someone can hack into your account and use your information ..."*
Contextual Conversations	Parents discuss privacy and security in context of a specific application rather than more broadly	*"I know they, they utilize the Facebook kids service ... and I have been very specific about what they ... should only use it for talking to their friends and that they shouldn't be putting any sort of other information online ... "*

I've done something similar to what it shows at the link. I think examples are really important... giving examples helps them make that distinction. So just examples via conversation." [P324]. One parent shared their strategy of showing phishing emails and texts they receive as teaching tools: "*So I've shared, I think from the perspective of when I get phishing emails, when I get phishing texts I will show them what they look like and they're like ... "* [P990]. This example demonstrated how parents integrated their own encounters with online privacy and security threats into family literacy conversations to foster shared awareness. Similarly, another parent shared how they took a hands-on example-based approach to show the child how to create a strong password: "*Ohhh yeah, definitely, I did teach my 8-year-old, if you gonna create an account, I mean let's just say he wants to create an Amazon account or gaming account, I told him always put a strong password, so, I tell him the combinations, the characters to use yes, so yes.*" [P724]. The use of concrete examples extended to scam identification as well. One parent recalled how they showed their children a fake PayPal email, shedding light on the deceptive tactics scammers employ: "*I showed them an email that I got that was like an Apple, like it was a scam, so I kinda showed them that email so they can see kinda how, it was PayPal, that's what it was, it was like a fake PayPal one.*" [P463]. This example-based approach allowed parents to offer insights into the nuances of potential threats that cannot be covered with conversation alone, and could potentially equip children with the ability to identify and navigate such situations on their own.

Overall, we saw parents experimenting with different ways to bring more tangible and illustrative examples of privacy and security literacy to children to communicate nuances of abstract privacy concepts, drive family conversations, and promote children's understanding of the complexities of the digital world.

4.3.3 ***Exposing Parents' Decision-Making Thought Process.*** Another conversational approach used by parents in our study involved parents exposing their own thought processes for digital privacy actions and decisions to their children. With this approach, instead of dictating rules, parents took the initiative to share their reasoning and rationale behind privacy-related choices with the hope of encouraging critical thinking and informed decision-making in their children. For example, one parent mentioned exposing their thought process of verifying if the website was secure before entering personal information: *"...if it's a game they're playing online I have to come up and use my credit card and then they see and I was like "okay now" so the first thing I'm doing is making sure this is a secure site, so I'm trying to show them what I do, to make sure that, or I was like, "where did you get this site from?" You know, "was it from the actual site or was it a you know, a link that was sent to you", so I'll ask those questions before I enter any of my, you know, credit card information. So hoping that, they're learning a little bit about that too."* [P313]. Parents also mentioned walking through scenarios with their children to illustrate how different pieces of

information could potentially be linked to uncovering one's personal details: "*Oh, there's a picture of you at a Dunkin Donuts, it could be the Dunkin Donuts between your home and your school and they could find you...this data.*" [P990]. By thinking aloud about the interconnectedness of information, parents intended to equip their children with a more comprehensive understanding of online exposure and how what they put online can be used by others.

In a similar way, parents also talked about openly discussing their own decision-making parameters when evaluating online situations for different contexts. One parent recalled a situation where their child wanted to share information online, and they detailed their thought process of how they were evaluating if the information should be shared on the platform under discussion or not: "*I'm like no you can't share information on that site... he asked me but they're his friends, and they play the video game together... and yeah because you only know these people and for the most part you probably ever wouldn't to see them they come next time it's going to be a different set of people playing that game are you going to share your content and pictures with every new gamer out there ...*" [P724]. This example showcased parents' attempt to invite the children into their thought process of making informed choices online rather than merely telling them dos and don'ts.

Parents also mentioned highlighting the importance of critical thinking in online interactions during their discussions with children. One parent discussed contextual questions they might ask their child to think about an online data sharing platform: "*Well, we've, we've told you she needs to address it with the person who's taken, who's taking the, who's taking the pictures, or who's posting online.*" [P669]. Moreover, parents also mentioned conveying their own experiences and concerns, sharing moments of uncertainty and how they navigate them with children. One parent mentioned, "*they hear me too. Sometimes I'll stress out about when I'm buying something and I'm like, "wait did I just get scammed," you know, then I start to... because I've learned this. This was just three weeks ago ... clicking on a link through Facebook no but, you know, it was a store through Facebook but then I bought something, and then afterward I was like, "why didn't I just go to the store directly ...*" [P313].

Overall, parents mentioned that they openly share and discuss their thinking process regarding digital privacy and security, as well as their ongoing learning journey as an educational approach to raise children's awareness of not only what actions to take, but also how they might want to think about different online situations.

4.3.4 ***Consequence-Based Conversations.*** In a consequence-based approach, parents actively engage their children in contemplating the potential risks or consequences of their online actions. Unlike example-based conversations that present tangible examples, consequence-based discussions leverage consequential thinking to motivate children to think about the potential risks of their online actions. Multiple parents mentioned how they explicitly tied online actions to potential outcomes to facilitate awareness of the unknown consequences that children might not be thinking about. For example, one parent discussed the implications of online posting without putting a thought into where you are posting, "*Yeah, I make them realize, you gotta be safe, you gotta be careful about what you put out there, cause you never know, you don't know who's watching you, you know, yeah so we do talk about it.*" [P724]. The same parent also described instructing their child about the importance of creating strong passwords, by emphasizing the risk of account hacking: "*I tell him hey if you don't create a strong password, someone can hack into your account and use your information ...*" [P724].

Additionally, we saw parents bringing in real-life instances and anecdotal stories to underscore the consequences of certain online actions such as sharing personal information. By recounting personal experiences, such as receiving unwanted calls due to shared information, one parent expressed to their children the tangible consequences of careless information sharing without considering the context: "*Even six or seven times they call me again, even the phone number is almost the same... he saw the result... when we share, yeah, that's the. He can have this maybe have even worse results.*" [P880]. Another parent built upon their child's day-to-day experiences to acknowledge the potential consequence of some of their seemingly innocuous actions of sharing pictures in a private group, as noted: "*Don't have people take photos of you, you know right. And the potential harm that something innocent, even if you're saying it in a private group chat, someone can take a screenshot. So I'm always kinda reiterating that part ...*" [P313].

Parents also tapped into real-life stories from various media formats, such as news articles or podcasts, to illustrate the potential consequences of online actions and enhance their children's awareness. For example, one parent discussed podcast stories as a means of educating their children about the potential repercussions of their online activities, where a student missed out on scholarships due to their social media posts: *"And I will especially want because of my kids' ages, I'll share stories like podcasts I hear of like a student not getting a scholarship because of something they posted on social media. And the possible impact of that.*" [P313].

Overall, this theme highlighted various ways in which parents tied online actions to their potential repercussions, such as linking weak passwords to the risk of account hacking and associating thoughtless online activities with the potential loss of scholarships, in order to help children become aware of far-reaching implications of their digital actions.

4.3.5 ***Contextual Conversations.*** Finally, the contextual conversations highlighted parent's approach of discussing online privacy insights in the context of specific applications and tailoring conversations to the platforms their children were using. This approach demonstrated a nuanced way in which parents more broadly discussed privacy considerations with children, focusing on privacy in specific application contexts. For instance, one parent mentioned discussing about privacy implications of Pokémon Go app: "*it's a game that my son recently asked me to download and I did allow him to download was that game Pokémon Go app, so that is one that I can think of in particular we had that conversation about.*" [P905]. Similarly, parents also mentioned deliberately guiding their children's use of specific platforms such as Facebook Kids: "*I have been very specific about what they should utilize that service for ... only use it for talking to their friends ... shouldn't be putting any sort of other information online ...*" [P324]. This approach highlighted parents' focus on setting clear boundaries within the context of a particular platform. During our study, we also saw parents acknowledging

the nuanced decision-making process that varies between different apps and scenarios. For example, one parent emphasized the importance of context, shedding light on differences in decision-making for location-sharing applications such as map versus another location tracking application: "*... the location tracking we've had a conversation about this actually we got into an argument ...because his dad said never do any like you always want to say no about like tracking. But then he downloaded like the map app. And you need to say where you are on the map app. So then he was super confused about that. So we had to have a conversation about the differences between those two things.*" [P810].

Overall, this theme illustrates how parents engage in conversations about online privacy that are tailored to the applications and platforms their children use, while also recognizing the potential complexities in these discussions that may emerge due to the contextual nature of different applications (e.g., location tracking within map versus social-media applications).

4.4 Which Type of Conversations Engaged Children?

During our analysis, we saw that parents' perceptions of children's engagement in discussions about online privacy and security differed based on their children's age (ages 10 and under versus ages 10+). Parents of younger children seemed to perceive their kids' participation in these conversations as closely tied to their understanding of the privacy concepts being discussed and its importance. For example, one parent mentioned their child questioning the rationale behind online privacy and security guidelines shared by parents: "*Yeah, I mean, I think the core question from them [the child] was, you know, why why, is this important? You know, why are you concerned about this?*" [P324]. This question reflects children's curiosity about the reasons behind their parents' concerns. Parents of younger children also acknowledged the challenge of explaining abstract digital privacy concepts to younger children. One parent mentioned that initially, young children displayed struggles to understand privacy concepts, however, as parents introduced real-world analogies into the conversation, children's engagement and comprehension improved. These analogies bridged the gap between the virtual and non-virtual worlds, helping children better grasp the significance of online privacy and security: "*Yeah, I think, initially, there was a reluctance and a lack of understanding... But I think as we kind of made that analogy and explained to them that the online device is really just an extension of the non-virtual world... there was greater understanding and engagement with the conversation.*" [P324]. At the same time, some parents also recognized that younger children might perceive digital privacy and security in relatively simplistic, black-and-white terms due to their limited understanding of abstract concepts, which could potentially hinder their ability to grasp nuances and discern when to share information online or respond to potential online risks. One parent expressed concern about their children's ability to fully engage in these conversations, stating, "*I don't think they do [engage in conversation], I really don't, that's the scary part, I think they can't... they're so black and white in their thinking, I don't know that they get the complete nuance of, you know when you send pictures... when you when it's appropriate to look online... I don't know that they fully get it, so.*" [P463].

In comparison to younger children, parents of older children often found that their attempts to engage their children in discussions about online privacy and security were met with varying degrees of resistance and disinterest. For instance, one parent reported that their children actively participated but often presented differing opinions and attitudes during these discussions: "*No, they're actively participating, but they're trying to engage on it with a differing opinion.*" [P523]. This suggests that older children may already possess their own perspectives on online privacy, leading to more interactive conversations, sometimes with disagreements. Many parents in our study mentioned that their older children, while physically present during these conversations, expressed disinterest, such as rolling their eyes and expressing a sense of already knowing what their parents were discussing. As one parent described, "*I think like participating they roll their eyes and are like, 'whatever mom okay, yeah I know.' But they don't really ask any questions or anything like that.*" [P810]. This disengagement indicated that some older children might consider these discussions repetitive or unnecessary.

Overall, this theme highlights different parent-child conversation dynamics among families of older versus younger children. The above findings highlight a need for more scaffolded and collaborative conversation opportunities for families with younger children to help children move beyond a black-and-white understanding of online privacy. For older children, since they already have some thoughts on online privacy and security, it is important to provide conversation opportunities that build on those disagreements and take things beyond what they already might know.

4.5 How Do Parents Think of Explaining Abstract Privacy and Security Concepts to Children?

During our study, we prompted parents to brainstorm ideas for educational interfaces that can help them explain abstract privacy and security concepts to children while engaging them in decision-making discussions. Parents shared a variety of ideas based on their experiences interacting with children at home. Some of these ideas focused on privacy learning interfaces that let children to *independently* learn about the nuances of privacy decision-making in different digital contexts, while other suggestions highlighted the need for *collaborative learning interfaces* for families that afford parent-child discussion opportunities.

In our analysis, one parent recommended **embedding privacy educational tutorials directly within children's applications**, such as gaming applications, to help children learn about privacy decision-making in different digital contexts either independently or collaboratively with their parents. This suggested approach highlighted the need for **adaptable and just-in-time lessons** across various digital contexts, enabling children or families to think about digital privacy and security before children use these applications: "*... I think that it may be helpful for platforms like apps to include tidbits about privacy and security to their gaming audience, you know, if we can assume that kids are going to have access to that particular game or application that there should be a perhaps a brief session*

or series of sessions as players advance in the game or as they log into the game quickly, you know, whether it's text or, you know, a combination of text and audio I think that that could be a really cool useful idea ... that you know could be effective." [P905]. Parents also suggested making these educational tutorials **interactive and gamified** rather than creating video-based or text-heavy lessons to foster children's engagement with the privacy literacy concepts: "*... it would be super cool like if they were playing an RPG ... gamify it for kids, you know, like I think there needs to be some type of like games some type of incentive some kind of fun and action something to motivate them to learn that and since ... I don't think that kids just sitting there and listening to somebody lecture like a podcast or whatever.*" [P905]. Another parent suggested the use of hands-on interactive classification games to teach children about **private versus personal information**, while also highlighting what could be considered private versus personal based on the application context: "*.... It could be some sort of game that involves classification, right? So it's going through various examples and asking them to click to classify it as personal versus private and then acknowledging to them when they're correct and incorrect.*" [P324]. As another example, the same parent suggested creating a **controlled "test environment" or sandbox** for children to help them learn consequences of different online interactions: "*Yeah, almost like a test environment had of one of these systems as well so that they can kind of a experiment in a sandbox, you know, if you will, before they actually delve into the actual, you know, live production system.*" [P324]. This environment could enable children to experiment safely when interacting with online applications and gain practical experience while avoiding the real-world risks linked with some online activities.

Parents in our study also highlighted the need for educational interfaces that offer parents and children "in-the-moment" discussion, reflection, and collaborative learning opportunities. This approach emphasizes parents and children learning and discussing privacy and security topics together rather than learning about them individually and discussing them later. We saw parents discussing the need for more collaborative learning materials that let both parents and children go through the experience together such as documentaries of real-life stories: "*But if there was like a something that we could watch together and then have a conversation afterwards I think that would be something that would interest me ...*" [P313]. One parent expressed an interest in an educational interface that allows parents not only to 'tell' but also to "show" their children the consequences of actions, such as using a weak password and account hacking, by **parents simulating unauthorized access** to the child's Facebook account during privacy-related discussions: "*I can pretend to get an access to your Facebook account, I can go down and type stuff that you don't wanna know, I can log to any of your accounts at these days pretty much anything we do revolve online, so, if anyone has access to your password, it's like somebody living at your home ...*" [P724]. Another parent mentioned discussing privacy and security literacy concepts as a family in informal learning settings such as church: "*Yes, so we usually, we discuss these [privacy and security] questions Hmm. yeah, in the with sister brother in church. We, yeah, we have the same age children. We can this, yeah, we sometimes we discuss about this question, with them and Yeah, we we have a lot of friends there. Yeah, we can discuss about that.*" [P880]. **Overall, a recurring theme in parents' suggestions was the emphasis on the importance of interactive and collaborative formats that engage children in understanding complex topics like online privacy as active participants, rather than passive recipients of information, and the need for interfaces that afford "in-the-moment" family discussion opportunities for both parents and children.**

5 DISCUSSION

In this section, we discuss our findings in relation to prior work and provide implications for designing privacy literacy interfaces for families.

Akter et al. [2] conducted a study with parents and teens exploring their mental models for a joint-oversight mobile application for teens' online safety and privacy. The authors noted that while software applications for direct communication between parents and teens might not be necessary, as they live in the same house, providing teens with indirect prompts to initiate offline discussions with their parents can still be beneficial. While teens might benefit from indirect discussion prompts [2], preteens require more engaging and hands-on approaches to understand and internalize digital privacy concepts [12]. Prior works by Muir and Joinson [18] and Williams et al.[31] delved into the broader aspects of how parents influence preteens' comprehension of online privacy and security concepts. Both of these studies concluded that, in comparison to device monitoring and usage restrictions, parent-child conversations play a crucial role in fostering a more nuanced understanding of digital privacy and security concepts among young children, and called for future research to gain an in-depth understanding of the nature of these parent-child conversations. Our paper takes a first step in response to this call for work and extends the prior work by providing a comprehensive insight into the structure of these parent-child conversations. We contribute a systematic categorization of five distinct types of parent-child conversations (**RQ1**): rule-based, example-based, expose decision-making process, consequence-based, and contextual conversations. This categorization could serve as a guide for researchers and designers of future family-centric privacy literacy technology interfaces to create more targeted interfaces that specifically support the types of conversations families are already having or need to have to facilitate the development of children's privacy and security decision-making skills.

Kumar et al. [14, 15] emphasized that privacy-focused educational resources for children should move beyond mere "dos and don'ts" and expose children to a spectrum of privacy consequences, in order to help them develop privacy-related decision-making skills. Our findings extend this prior work by providing empirical insights into the dynamics of parent-child conversations that have not been explored in the literature yet. We found that parents often employed a combination of conversational approaches, with rule-based conversations being one of the most common methods. Our findings also showed the potential of example-based conversations as being perceived effective in helping children develop privacy literacy. In the rule-based approach, parents instructed children about specific rules (e.g., don't share personal data online or don't share location) to follow when online, with the "hope" that children would remember and apply these rules across multiple platforms

and applications. This inclination towards a rule-based conversational approach could be related to parenting styles [18, 30], which in prior work has been used to describe how parents mediate their children's use of media, such as controlling styles (imposing rules), autonomy-supportive styles (explaining the reasons behind rules while considering the child's perspective), and inconsistent styles (enforcing rules inconsistently). Alternatively, parents resorting to a rule-based approach may also stem from their perception of their knowledge regarding privacy and security. Some parents may not consider themselves experts in explaining these abstract concepts to children, as indicated by one of our study participants: "*I feel a lack of resources or knowledge of parents of how to navigate especially with kids that know to just create other Gmail accounts like I don't know like what are, what are our options there.*" [P313].

We also explored parents' perceptions of children's engagement during parent-child privacy and security literacy conversations (**RQ2**). Overall, we saw different patterns in parents' perceptions of how older (ages above 10) versus younger children (10 and under) engaged during these conversations. Parents in our study discussed older children's tendency to be less receptive to the privacy conversations initiated by their parents, sometimes leading to disagreements. On the other hand, parents perceived younger children demonstrating a greater willingness to participate in these conversations, often inquiring about the rationale behind parents' online privacy concerns and recommendations. Parents in our study acknowledged the challenge of explaining abstract digital privacy concepts to younger children. They discussed the importance of bridging the real world and the virtual world to help children move beyond a simplistic, black-and-white understanding of online privacy and security to a more context-based approach. To do so, future work on designing privacy educational interfaces can draw on theories like Contextual Integrity [20], which emphasizes five contextual elements to consider during privacy decision-making, including the social context where decisions are made, the sender and recipient actors involved, the type of information being shared, and the principles of information transmission used to transfer information among actors [19, 20]. By incorporating Contextual Integrity theory into the design process of privacy literacy interfaces [14], these educational tools can provide children with an experiential understanding, enabling them to make more informed privacy decisions by leveraging the context and going beyond rule-based knowledge.

5.1 Design Implications for Privacy and Security Literacy Technologies

Based on our findings, we offer design implications for family-centered privacy and security literacy technologies (**RQ3**).

5.1.1 ***Consider incorporating tangible examples and visualizations within privacy and security literacy applications for families.*** Beyond the rule-based approach, we observed example-based conversations where parents experimented with different ways to incorporate tangible and illustrative examples of privacy and security literacy into their discussions with children. For instance, they used examples of phishing emails and text messages to help convey the nuances of abstract privacy concepts and facilitate family discussions. Prior work in learning sciences [28] has discussed how tangible examples and visualizations can help students grasp abstract concepts by making them concrete, enabling children to understand what they cannot see otherwise. Parents in our study found the example-based conversation approach effective in conveying information and engaging children during discussions. Based on this finding, we recommend that designers consider incorporating tangible examples and visualizations within privacy literacy applications designed for families; this could provide parents with effective discussion starting points based on the provided examples. For example, these applications could simulate real-world situations, such as a platform that prompts children to differentiate between sharing personal (e.g., likes or dislikes) and private information (e.g., location or name) in various digital contexts and provides feedback. Another approach could involve a simulated email inbox with phishing emails, allowing children to interact with and learn from examples.

5.1.2 ***Explore the effectiveness of consequence-based conversational approaches for younger children's privacy literacy.*** In our analysis, we observed that parents employed consequence-based conversational approaches to illustrate the potential risks associated with various online actions. This finding aligns with the research conducted by Williams et al. [31], who found that multiple parents in their study mentioned explaining the consequences of poor online choices and decisions to children. The approach of parents emphasizing consequences, also known as the 'why-because' method, has been shown to be effective in aiding preschool children in developing general consequential thinking skills [9]. Consequential thinking refers to the ability to consider the potential outcomes of one's actions before making decisions, more broadly (e.g., understanding that the consequence of not eating lunch is being hungry). None of the parents in our study discussed the effectiveness of this conversational approach in the context of privacy literacy. Although the effectiveness of consequence-based conversations is shown in other general contexts, it might differ when applied to privacy literacy, especially for young children. It is important to note that younger children often have difficulty conceptualizing privacy and security concepts, let alone understanding the implications of those actions. As a result, young children may find it difficult to connect online actions with consequences. Therefore, more work is needed to evaluate the effectiveness of consequence-based conversational approaches for younger children who are still developing their understanding of privacy and security concepts. It would be interesting to see which type of conversations work best based on children's age group and use this understanding to inform the design of privacy literacy education technologies for children.

5.1.3 ***Support synchronous collaborative learning interfaces for families.*** Parents in our study noted that children, especially younger ones, tend to perceive privacy and the digital world in a simplistic, black-and-white manner. While children of all ages are familiar with basic privacy and security terminology [15, 31], in our study parents perceived that their understanding often lacks nuance and the ability to consider different contexts. To foster a more sophisticated understanding, parents emphasized the need for educational interfaces that facilitate joint learning experiences for both parents and children. This collaborative approach would enable parents and children to explore privacy literacy concepts

together, rather than having children and parents learn separately and then attempt to discuss these concepts later. This collaborative approach may offer several benefits, including enabling children to ask questions, allowing parents to gain insight into their children's mental models, and providing a scaffolded space for parents to have a deeper discussion about applying privacy concepts in different contexts. Parents suggested a range of learning resources to support this collaborative learning approach, including documentaries that focus on real-world privacy and security stories relevant to children. Additionally, parents advocated for interactive learning environments designed for families where children can act, fail, and learn from their decisions. These environments can also provide parents with opportunities, thoughtful questions, or prompts, to engage in meaningful conversations about privacy concepts. For instance, one parent proposed the idea of a "sandbox" environment where children could experiment with different actions and observe the resulting consequences. In this scenario, parents would play a guiding role, offering support and guidance to help children make informed decisions in various situations. Therefore, based on this finding we recommend researchers and designers to explore ways to design privacy literacy interfaces that support both parents and children together in an interactive learning process, and more intentionally embed opportunities for discussions through task prompts or questions.

6 CONCLUSION

We report an analysis of interview data with 13 parents reflecting on their privacy literacy practices at home. We contributed a systematic categorization of five privacy- and security-related parent-child conversations: rule-based, example-based, exposing decision-making, consequence-based, and contextual conversations, and uncovered parents' perceptions of children's engagement during these conversations. Overall, We found that parents often employed a combination of these conversational approaches, with rule-based conversations being one of the most common methods and example-based conversations perceived to be effective for young children. Based on our findings, we present new recommendations for designing privacy and security literacy technologies tailored for families that foster more engaging and collaborative privacy discussions between parents and children.

ACKNOWLEDGMENTS

We thank Dr. Mohan Zalake, Anupreeet Paulkar, and Parth Kirankumar Thakkar for their help with this work; and anonymous reviewers for their constructive feedback.

REFERENCES

[1] Mamtaj Akter, Leena Alghamdi, Jess Kropczynski, Heather Richter Lipford, and Pamela J. Wisniewski. 2023. It Takes a Village: A Case for Including Extended Family Members in the Joint Oversight of Family-based Privacy and Security for Mobile Smartphones. In *Extended Abstracts of the Conference on Human Factors in Computing Systems (CHI'EA 23)*. 1–7.

[2] Mamtaj Akter, Amy J Godfrey, Jess Kropczynski, Heather R Lipford, and Pamela J. Wisniewski. 2022. From Parental Control to Joint Family Oversight: Can Parents and Teens Manage Mobile Online Safety and Privacy as Equals? *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW1 (2022), pp. 28.

[3] Ann Blandford, Dominic Furniss, and Stephann Makri. 2016. *Qualitative HCI research: Going Behind the Scenes*. Morgan & Claypool Publishers.

[4] Victoria Clarke and Virginia Braun. 2013. Successful Qualitative Research: A Practical Guide for Beginners. *Successful Qualitative Research* (2013), 1–400.

[5] Katie Davis and Carrie James. 2013. Tweens' Conceptions of Privacy Pnline: Implications for Educators. *Learning, Media and Technology* 38, 1 (2013), 4–25.

[6] Tom De Leyn, Ralf De Wolf, Mariek Vanden Abeele, and Lieven De Marez. 2022. In-between Child's Play and Teenage Pop Culture: Tweens, TikTok & Privacy. *Journal of Youth Studies* 25, 8 (2022), 1108–1125.

[7] Common Sense Education. 2021. Privacy and Security: Family Tips for K-5. https://www.commonsense.org/education/family-tips/k-5-privacy-and-security Accessed: 10-14-2021.

[8] Common Sense Education. 2023. Digital Citizenship Curriculum. https://www.commonsense.org/education/digital-citizenship/curriculum?topic=privacy--security Accessed: 04-26-2023.

[9] Maurice J. Elias. 2023. *Teaching Young Children to Understand Consequences*. https://www.edutopia.org/article/explaining-consequential-thinking-young-children Accessed: 09-11-2023.

[10] Steven Furnell and Emily Collins. 2021. Cyber Security: What are We Talking About? *Computer Fraud & Security* 2021, 7 (2021), 6–11.

[11] Arup Kumar Ghosh, Charles E Hughes, and Pamela J Wisniewski. 2020. Circle of Trust: A New Approach to Mobile Online Safety for Families. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI'20)*. 1–14.

[12] Yasmeen Hashish, Andrea Bunt, and James E Young. 2014. Involving Children in Content Control: A Collaborative and Education-Oriented Content Filtering Approach. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI'14)*. 1797–1806.

[13] Hilary Hutchinson, Wendy Mackay, Bo Westerlund, Benjamin B Bederson, Allison Druin, Catherine Plaisant, Michel Beaudouin-Lafon, Stéphane Conversy, Helen Evans, Heiko Hansen, et al. 2003. Technology probes: Inspiring Design for and with Families. In *Proceedings of the Conference on Human factors in Computing Systems (CHI'03)*. 17–24.

[14] Priya Kumar and Virginia L Byrne. 2022. The 5Ds of Privacy Literacy: A Framework for Privacy Education. *Information and Learning Sciences* 123, 7/8 (2022), 445–461.

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

[16] 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 *In Proceedings of the Conference on Interaction Design and Children (IDC'18)*. 67–79.

[17] MediaSmarts. 2019. Helping Kids Navigate the Digital World. https://mediasmarts.ca/sites/default/files/guides/guide_helping_kids_navigate_digital_world.pdf

[18] Kate Muir and Adam Joinson. 2020. An Exploratory Study into the Negotiation of Cyber-security Within the Family Home. *Frontiers in Psychology* 11 (2020), Article 424.

[19] Helen Nissenbaum. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

[20] Helen Nissenbaum. 2019. Contextual Integrity Up and Down the Data Food Chain. *Theoretical Inquiries in Law* 20, 1 (2019), 221–256.

[21] U.S. Department of Health and Human Services. 2021. Preventing Cyberbullying in the Age of Smart Phones. https://www.stopbullying.gov/blog/2021/07/29/preventing-cyberbullying-age-smart-phones. Accessed: 2023-04-26.

[22] UK Ofcom. 2019. Children and parents: Media use and attitudes report 2018. *Ofcom Website: London, UK* (2019).

[23] Farzana Quayyum, Daniela S Cruzes, and Letizia Jaccheri. 2021. Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction* 30 (2021), 100343.

[24] Kate Raynes-Goldie and Matthew Allen. 2014. Gaming privacy: A Canadian case study of a co-created privacy literacy game for children. (2014).

[25] Janet C Read and Russell Beale. 2009. Under my pillow–designing security for children's special things. *People and Computers XXIII Celebrating People and Technology* (2009), 288–292.

[26] Victoria Rideout. 2011. *Zero to Eight: Children's Media Use in America*. Common Sense Media.

[27] V Rideout, A Peebles, S Mann, and MB Robb. 2022. Common Sense census: Media Use by Tweens and Teens, 2021. Common Sense.

[28] David F Treagust. 2008. The role of multiple representations in learning science: enhancing students' conceptual understanding and motivation. In *Science education at the nexus of theory and practice*. Brill, 7–23.

[29] UNICEF. 2021. Violence Against Children Online. https://www.unicef.org/protection/violence-against-children-online. Accessed: 2023-04-26.

[30] Patti M Valkenburg, Jessica Taylor Piotrowski, Jo Hermanns, and Rebecca De Leeuw. 2013. Developing and Validating the Perceived Parental Media Mediation Scale: A Self-determination Perspective. *Human Communication Research* 39, 4 (2013), 445–469.

[31] Olivia Williams, Yee-Yin Choong, and Kerrianne Buchanan. 2023. Youth understandings of online privacy and security: A dyadic study of children and their

parents. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS'23)*. 399–416.

[32] Christina L Wissinger. 2017. Privacy literacy: From Theory to Practice. *Communications in Information Literacy* 11, 2 (2017), 378–389.

[33] 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 (IJCCI'17)* 13 (2017), 10–18.

[34] Leah Zhang-Kennedy and Sonia Chiasson. 2021. A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Computing Surveys (CSUR)* 54, 1 (2021), 1–39.

[35] 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 Conference on Human Factors in Computing Systems (CHI'19)*. 1–13.