Exploring Design Opportunities for Family-Based Privacy Education in Informal Learning Spaces

Lanjing Liu
lanjing@vt.edu
Virginia Tech
Blacksburg, Virginia, USA

Lan Gao
langao@uchicago.edu
University of Chicago
Chicago, USA

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

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

ABSTRACT

Children face increasing privacy risks and the need to navigate complex choices, while privacy education is not sufficient due to limited education scope and family involvement. We advocate for informal learning spaces (ILS) as a pioneering channel for family-based privacy education, given their established role in holistic technology and digital literacy education, which specifically targets family groups. In this paper, we conducted an interview study with eight families to understand revealing current approaches to privacy education and engagement with ILS for family-based learning. Our findings highlight ILS's transformative potential in family privacy education, considering existing practices and challenges. We discuss the design opportunities for family-based privacy education in ILS, covering goals, content, engagement, and experience design. These insights contribute to future research on family-based privacy education in ILS.

KEYWORDS

Privacy education, children, family groups, informal learning spaces

1 INTRODUCTION

Children (6-14 years old) are getting more attached to various technologies, from social media to handheld electronic devices, to wearable devices and other emerging technologies. Yet, their privacy knowledge and their ability to make informed privacy decisions do not match with technological advancement. Research has suggested that while children have a basic understanding of fundamental terminologies, they lack essential knowledge and ability to foster decision-making skills and take responsible digital behaviors [92]. For example, children are often asked to follow certain rules [48], yet the rule-based approach oftentimes does not suffice the varying privacy needs given the contextual nature of privacy [68].

As such, researchers have been exploring different means to carry out privacy education for children to improve their privacy knowledge and foster their skills to make informed privacy decisions. For example, an interactive medium is designed to foster early adolescents' awareness of information privacy in their everyday online practices [96]. There are also some games designed to develop children and teenagers' privacy literacy [60, 72].

However, we believe that these existing practices of privacy education are limited mainly in the following three ways. First, most privacy education practices predominantly focused on online privacy education [29, 93, 99] and thus were not effective in addressing privacy risks in the offline space or in the intersection of online and offline contexts. This is particularly important considering children's increasing engagement with various cyber-physical devices that span across both real-world and online spaces (e.g., smart home devices, virtual reality, augmented reality, etc.), which were known for posing significant privacy risks to their users [1, 52, 95]. Secondly, current privacy education approaches focus on addressing privacy issues through one-time, short educational activities (e.g., using mobile applications [105] or interactive e-books [103]) rather than improving children's privacy literacy. As a result, these approaches fall short of generating a long-term impact on children's privacy knowledge and behavior. Thirdly, existing privacy education approaches primarily target individuals through school learning or self-learning [26, 47, 71, 98] and do not leverage their immediate family members in this process [63]. Such omission could negatively impact their family members' ability to guide their children in making privacy decisions [59].

In searching for ways to bridge these gaps, we noticed that the HCI (Human-computer interaction) community has extensively explored utilizing informal learning spaces (ILS), such as museums, science centers, libraries, for technology and digital literacy education [42, 55], many of which target family groups, a prevalent demographic in these settings [28, 39, 67]. This line of research inspired us to think, is it possible to utilize ILS for family-based privacy education to improve children's privacy literacy?

As privacy researchers and educators, our goal is to explore a novel, **family-based privacy education approach in ILS**. As family often experiences enriched interactions in informal learning settings [31, 64, 77], we aim to build interactive, privacy-centric exhibits or artifacts and display them in various ILS. Ideally, interacting with these exhibits or artifacts would spark family-based discussions around privacy and expose several "teachable moments"

Proceedings on Privacy Enhancing Technologies YYYY(X), 1–17

https://doi.org/XXXXXXX.XXXXXXX

for us to inject relevant privacy education materials for deeper learning.

However, this novel approach at the intersection of family-based privacy education and informal learning has not been studied in the literature. On the one hand, it is not clear how families go about privacy education especially considering the possible imbalanced power dynamics and conflicted interests, hindering the collaborative practices of addressing privacy concerns [9, 41, 54, 104]. On the other hand, it is also not clear how families utilize public infrastructure in ILS for interactive learning.

In this paper, we present an initial exploration of the design opportunities for family-based privacy education in ILS. In particular, we focus on the following research questions:

- RQ1: How do families conduct privacy education, and what are the characteristics and challenges involved?
- RQ 2: How do family groups utilize ILS for interactive learning?
- RQ 3: What design opportunities exist for providing privacy education within ILS?

To answer our research questions, we conducted an interview study with eight families. Each family includes a parent and a child (age 6-14, a critical age range where they can understand privacy concepts [20]). The interviews focused on the roles that each family member played in privacy learning, the learning approaches, the challenges, as well as the common practices of utilizing public infrastructures in ILS for interactive learning. Our findings highlighted the characteristics of existing family-based privacy education, such as the multiple roles played by children, the prevalence of open conversations as a medium for privacy education, and the occurrence within specific contexts, as well as challenges, such as privacy tensions among family members, the complex contextual nature of privacy, and a deficiency in comprehensive knowledge among all family members. In the meantime, our results also suggested the positive outcomes when utilizing ILS for interactive learning. In the discussion, rooted in our empirical evidence, we re-iterated why family-based privacy education in ILS could be a promising direction to enhance children's learning of privacy, then drew design implications for effective education outcomes.

Our paper makes three contributions: First, we proposed a novel approach for privacy education, suggesting integrating privacy education within ILS and providing design opportunities. Second, we conducted an exploratory study to investigate the current privacy education practices and tensions within families as well as how families engage and learn within ILS, particularly regarding technology-related topics. Third, we discussed the design opportunities and drew design implications for effective, family-based privacy education in ILS.

2 RELATED WORK

2.1 Privacy Challenges in Family

2.1.1 Lack of privacy awareness and knowledge. Traditionally, both parents and children in families have demonstrated weak privacy awareness and knowledge. Parents often share personal details and family photos on social media, potentially revealing their children's information to a broad online audience [2, 7, 33, 62, 81]. When using smart home or voice assistants at home, many individuals demonstrate blind trust in manufacturers, assuming they are not potential targets, and tend to overlook certain privacy risks [100, 107]. Unsurprisingly, children are generally not aware of the privacy risks they may face, such as online tracking or game promotions [106], identity re-identification [70], except some basic privacy risks, such as information oversharing or revealing real identities online [104].

2.1.2 Multi-member families and relationships. As a family typically involves various members — parents, relatives, children, and visitors, it raises privacy concerns related to imbalanced power dynamics, privacy permission, and confidentiality.

Imbalanced power dynamics and interdependence of privacy are fairly common in a family setting. For example, family locator apps commonly acquire family members' location information and contact details, some applications even allow the designated family controller to remotely access the camera or microphone of other family members [4, 50]. Parents also monitor children's physical activity and sleep via wristbands, leading to conflicts between parents and children [44]. Another context for imbalanced power dynamics within family groups relates to the use of social media. Parents posting photos and other information about children on social media is common [6, 10, 46, 65]. Yet this sharing behavior raises issues of consent between the sharer (such as parents or other adults) and the recipients (especially children, or other family members) [41]. Different children have varying attitudes towards this sharing behavior, often expressing reluctance to have their private information or actions shared on public social networks [41, 43, 66]. In the home setting, robots are faced with dynamic locations and unique interactions with different family members, which exposes each individual's private information to the threat of being compromised by the manufacturer and other family members [27, 32, 53]. Many kids do not realize parents can access their audio recordings via smart toys or household robots. Older children often worry about their privacy being invaded by their parents through these devices [61]. Finally, while there are attempts to address imbalanced power dynamics and interdependence in privacy [19], very few of them specifically target family members to raise awareness of this inequality.

2.2 Privacy Education

Literature has suggested two main forms of interventions aimed at cultivating awareness of privacy for children: games and interactive e-books. Generally, these games and interactive e-books allow children to understand and choose basic questions about privacy, such as tracking cookies, personal data on social media, etc., and to make sound judgments within prescribed scenarios [47, 71, 72, 96, 97]. Some research also specifically focuses on the privacy conflicts between parents and children, aiming to help parents better handle their children's online privacy. For example, *Circle of Trust* provides a new method of controlling online privacy for families by valuing privacy, trust, freedom, and balance of power preferred between children and parents [36].

These educational efforts use a one-way approach, which may face inherent limitations. For example, it struggles to effectively guide children in applying their privacy knowledge across various contexts given the complexity of real-life privacy issues and

contexts children may encounter. Additionally, the efforts miss the opportunity to involve parents and other family members in privacy education activities. When adults are involved, they can acquire the necessary knowledge and skills themselves and guide their children in understanding and effectively addressing privacy challenges. Our proposed approach aims to fill this gap.

2.3 Informal Learning Spaces and Family Group

Informal learning spaces have long served an important role in public education efforts, including places like museu ms [31, 84, 91], libraries [83], and science centers [45, 74, 76]. Also, consideration of family-based groups in museums and other informal learning spaces is widely acknowledged and implemented as part of their educational obligations [5, 39, 57, 67].

2.3.1 Informal Learning Spaces and Technology-Related Education. In the Human-Computer Interaction (HCI) and Computer-Supported Cooperative Work (CSCW) communities, there have been many efforts to explore using informal learning spaces for educational purposes. These efforts focus on computer science and digital literacy education, such as programming [42], computing concepts [56], and AI literacy [57]. There are several broadly applicable design features to consider when designing learning experiences in informal learning spaces. For example, tangible and interactive interfaces can enhance understanding of concepts [64, 85]. They also promote a resonance with others through bodily experiences [58, 77]. Open-ended exhibits encouraging creativity lead to extended engagement, enabling visitor-driven learning and fostering personally meaningful interpretations [12, 31]. This, in turn, supports the application of acquired knowledge to develop individualized privacy management systems in everyday technology usage. Other technologies and interactive features are employed in informal learning spaces, such as museums, to enhance people's experiences. Examples include virtual reality (VR) [78, 102], augmented reality (AR) [13], IoT [87]. These technologies and interactive elements are designed to engage visitors and provide immersive and interactive learning opportunities. For example, Long et al. conducted an exploration of AI literacy in museums [57]. They specifically focused on families as their target user group, acknowledging the prevalent occurrence of family visits in museums. Moreover, they recognized that many parents may lack the requisite AI literacy, thereby impeding their capacity to effectively educate their children on relevant knowledge. The situation of privacy literacy is similar to that of AI literacy. Inspired by this line of research, we consider informal learning spaces such as museums as one of the key scenarios for improving people's privacy literacy, which allows family groups to understand privacy in technology and learn to manage the privacy issues of various devices and platforms.

2.3.2 Family-Based Groups in Informal Learning Spaces. Research on family-based informal learning recognizes the importance of interactions among family members, particularly parents and children, during their visits [86]. Previous studies have identified parent-child interaction within informal contexts as a pivotal mechanism for facilitating learning [14]. Conversations within family groups are a common form of interaction among family members and typically span the entire process of visiting. Through explanations, associations, and open-ended questions, these conversations support learning and the formation of meanings [17, 37]. In family conversations, parents often serve as "translators" for their children [108], and the learning process often occurs as parents provide structure to their children's understanding based on their experiences [8, 22, 38]. There have been many researches that promote interaction between family members. Signage and parallel information can also be designed to promote family communication and awareness [51, 108]. Engaging in inquiry games, especially the ones that involve the whole family, has been shown as an important means of promoting family learning in informal learning spaces [37].

While previous studies acknowledge the potential of informal learning spaces for family-based learning, they often do not address the unique challenges associated with incorporating privacy education. By examining the interactions, practices, and experiences of families in these environments, we seek to design and implement effective privacy education programs tailored to the unique dynamics of informal learning settings. Our research extends the current understanding of how families interact with educational content within informal learning spaces.

3 METHODOLOGY

To inform the design of family-based privacy education interfaces in informal learning settings, we conducted a semi-structured interview study to understand (1) families' existing practices to address privacy challenges and carry out privacy education, and (2) how families utilize informal learning spaces for family-based learning. This study is approved by our university's IRB.

3.1 Participants Selection

As our study focuses on family-based privacy education, we aim to look for families that meet the following criteria: (1) the family must have a child between the ages of six and fourteen; (2) the child in the family should have some experience with intelligent technologies and the Internet; (3) the families should have prior experiences visiting one of the following places: museums, science centers, zoos, aquariums, botanical gardens, nature centers, or historical sites; and (4) each family should have at least one child and one parent present during the interview session.

We chose children between six and fourteen for three reasons: (1) children would not start to develop the cognitive ability to comprehend and engage with complex concepts such as privacy until the age of six [20, 34, 90]; (2) psychologically, children between the ages of six and fourteen are at a critical time of development to acquire a wide range of knowledge and skills which may further influence their behaviors and decision-making processes [80];

We recruited our participants mainly by posting our recruitment materials on social media (e.g., Twitter and Facebook), then used snowball sampling on the selected participants (i.e., we asked the participants to help us identify other families interested in participating in our research). In total, we interviewed eight families, with one parent and one child in each family group. They represented a wide range of backgrounds, ages, and geographic locations. The details can be found in the Table 1.

ID	Age	Gender	Education	Employment Status	Location	Informal Learning Spaces	Frequency	Specific Names
P01	35-44	Male	Bachelor's	Full-time	Western US	Museums, Science Centers, Historical Sites, Libraries	Occasionally	Local Museum of Arts, Local Science Center, Local Library
C01	12-14	Male	7th-9th	N/A				
P02	25-34	Non-binary	Bachelor's	Full-time	Eastern US	Museums,Science Centers,Libraries	Occasionally	Local Science Gallery, Local Library, National Museum, National Library
C02	12-14	Male	7th-9th	N/A				
P03	35-44	Male	Bachelor's	Full-time	Midwest US	Museums, Science Centers, Historical Sites, Libraries	Occasionally	Local Cultural Center, Local Museum of Science and Industry
C03	12-14	Male	7th-9th	N/A				
P04	35-44	Male	Graduate	Full-time	Western US	Museums, Science Centers, Nature Centers, Libraries	Occasionally	Local Science Center
C04	9-11	Male	4th-6th	N/A				
P05	35-44	Female	Bachelor's	Homemaker	Western US	Museums, Science Centers, Nature Centers, Historical Sites, Libraries	Occasionally	Discovery Cube, Missions, Local Natural Museum, Local Science Center
C05	12-14	Female	7th-9th	N/A				
P06	45-54	Male	Graduate	Full-time	Western US	Museums, Science Centers, Nature Centers, Libraries	Rarely	National Park
C06	12-14	Female	7th-9th	N/A				
P07	35-44	Female	Graduate	Full-time	Western US	Museums, Science Centers, Nature Centers, Libraries	Frequently	Local Aviation Museum, Libraries
C07	6-8	Male	1st-3rd	N/A				
P08	35-44	Female	Graduate	Homemaker	Western US	Museums, Science Centers, Nature Centers, Historical Sites, Libraries	Occasionally	Local Science Center, Discovery Cube
C08	6-8	Male	1st-3rd	N/A				

Table 1: Participants demographics. In the "ID" column, P refers to a parent and C refers to the child from the same family. "Frequency" refers to how often participants visited informal learning spaces, with "Rarely" meaning a few times a year, "Occasionally" meaning a few times a month, and "Frequently" meaning once a week. "Specific Name" refers to the informal learning spaces the participants enjoyed

3.2 Interview Protocol

To account for the two different participant groups, we prepared two interview protocols, one for the parents and one for the children. The interview questions were consistent in both versions, although certain phrasings were modified to ensure comprehension by the children [69]. We used the parents' interview protocol as an example.

The interview protocol contains three sections. The first section focused on the participants' experiences and concerns regarding privacy issues within the family context, as well as their current practices in mitigating these issues. Sample questions include "*have you encountered any privacy-related situations or dilemmas within your family?*", "*Have there been any conflicts among your family members regarding privacy?*", and "*What measures do you or your family usually take to address privacy issues?*". The second section focused on the specific needs of family members concerning learning and managing privacy. Sample questions include "*How do you handle situations where your child's privacy is violated or compromised?*" and "*What are your hopes or expectations regarding privacy within your family?*" Finally, in the third section, we focused on their experiences in ILS and asked questions such as "*Have you engaged in studying or learning activities with your children outside of school?*" and "*What activities do you typically engage in with your children during these moments?*" We also asked participants to discuss whether these ILS could be used for privacy education purposes, and if so, how. The complete interview protocols for both parents and children can be found in the Appendix A.1.

3.3 Interview Procedure

All interviews were conducted over Zoom from August 2023 to October 2023. Parents and children were interviewed separately. Only one parent chose to observe the interview by sitting next to the child (the parent went first). All other interviews were done with either the child or parent individually. The order was decided by

participants (children first: 3; parents first: 5). When the interviews started, parents were asked to read and sign the consent form while children were asked to read the consent and assent forms together with their parents, then sign them. Next, we proceeded with the interview questions and asked follow-up questions as needed. Each interview was conducted by two co-authors, with one primarily asking the questions while the other focusing on note-taking. Interviews with parents lasted from 30 to 55 minutes (average: 43 minutes), and interviews with children ranged from 23 to 59 (average: 42 minutes). Upon completion, each participant received a compensation of $20 (i.e., the family group with one parent and one child would receive $40). We reached saturation after 7 families and stopped recruiting after the eighth family. This is partially because children tend to answer questions briefly.

3.4 Data Analysis

The transcriptions from Zoom were carefully checked and corrected by the co-authors, then analyzed using an inductive analysis approach, which is largely informed by the thematic analysis methodology [15]. The analysis was done iteratively in several steps. After the first four families, we conducted a preliminary analysis to identify areas requiring further data collection and refine the interview protocol. We repeated this process for the remaining interviews, ensuring a continuous and iterative reflection on the interview questions.

Upon the completion of data collection, we followed the thematic analysis procedure. Two co-authors read the interview transcripts several times and coded data from two families (four interviews in total) collaboratively and generated two initial codebooks (one for children and one for parents). Using the initial codebooks, the two co-authors coded the rest of the data individually. They constantly compared and discussed their codes and resolved any disagreements as they coded, then updated the codebooks as needed. Upon completion of the coding, the two co-authors cross-checked each other's coding again to ensure full agreement. Then, the co-authors examined and discussed the codebooks, then grouped the codes into higher-level themes. The final codebooks for parents and children contain 138 unique codes in 11 themes and 149 unique codes in 10 themes, respectively.

Given the qualitative nature of this study, we avoided reporting the exact number of examples and themes. Instead, we adopted a consistent terminology to convey the relative sense of the frequency of major themes [30, 101], as illustrated in Figure 1.

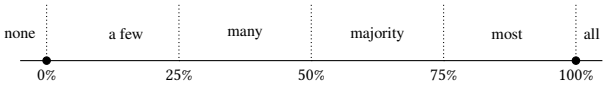

Figure 1: Our terminology to describe theme frequencies

3.5 Interview Research Ethics

As our research involved minors between the ages of six and fourteen, we paid extra attention to our research ethics. First of all, we ensured that all parents and children were well informed of the study procedure, their rights, and measures they could take when withdrawing from the study was desired. Second, similar to McReynolds et al. [61], interviews with parents and children were conducted separately. This was to avoid interference and possible awkwardness between parents and children. To ensure the transparency of interviews and reduce the safety concerns of the parents, similar to Sun et al.'s work [82], parents were allowed to observe their children's interviews if they wished to. Finally, we took the following measures to ensure the confidentiality of participants' sensitive personal information: (1) during the interviews, we consistently reminded participants to focus on their own experiences and opinions and not reveal private or sensitive information throughout the interviews; (2) we stored and handled data securely, used pseudonyms or participant codes instead of real names, and anonymized any identifiable information during analysis and reporting; (3) for our children participants, we employ child-friendly language to remind them not to share sensitive information. We reflected on our methodology in the Section 5.3.

3.6 Limitations

There are various limitations in our study. First, we only interviewed eight families, including eight children and eight parents. While we believe that our sample size was sufficient for our study, we recognized that there may be other types of privacy challenges experienced by other family groups. Second, as with any qualitative research, the subjective nature of individual experiences and interpretations may introduce biases and limitations. While we tried to encourage open sharing, participants' responses may still be influenced by social desirability or other personal factors. Finally, our study was conducted within a specific cultural and societal context (i.e., the US context), and the findings may not be directly applicable to different cultural or geographical settings, acknowledging that the privacy challenges and experiences within families could vary across different communities and contexts [73, 75]. Further research is needed to explore these variations.

4 RESULTS

4.1 Characteristics of Existing Family Privacy Education

In general, parents perceived privacy as important as other schoolwork and skills for their children. Our data suggested that all participating families had engaged in some type of privacy-related educational activities or discussions. From the children's perspective, most children also showed an open attitude towards privacy education. The majority of children actively explored various methods for managing their privacy and expressed a desire for more support. Upon further analysis, the discussion of privacy and the practices of privacy education within family groups demonstrated several unique characteristics as presented below.

4.1.1 Children Played Multiple Roles in Privacy Education. In family-based contexts, children's engagement in learning about privacy has been largely expanded, thus playing multiple roles.

Children as a Vulnerable Group. Due to children's limited ability to identify privacy risks and carry out meaningful privacy protections, the majority of parents considered their children to be vulnerable. As a result, many parents, instead of teaching their

children about privacy and increasing their privacy literacy, opted to actively protect their children's privacy with proactive actions.

Similar to prior work [48], many parents in our study took precautionary measures and set up certain rules for their children, such as not inviting strangers into their homes and refraining from disclosing their SSN and birth date to others. Furthermore, some parents tried to limit their children's Internet or smartphone usage to reduce online privacy risks and other issues, such as addiction and exposure to inappropriate content. Their measures included opting for lower-speed Internet services (P06, 45-54, M), assigning children's free time to homework or outdoor activities (P05, 35-44, F), using parental control services to limit their children's Internet access (P02, 25-34, Non-Binary), only permitting Internet access through shared family computers (P04, 35-44, M), etc. Similar to the findings in prior work [89], the majority of parents in our study also admitted that they regularly checked in with their children to ensure they were safe, which included monitoring their children's use of social media (P01, 35-44, M) and supervising their private communications with mutual consent (P06, 45-54, M).

Children as Active Learners. In our study, most children were also active learners. In this role, parents tended to embrace their children's ability to learn new concepts and perform various types of privacy education. From the children's perspective, they acquired privacy-related knowledge through family educational activities, including general activities and privacy-focused education. Such education included different types of privacy, such as body/physical privacy, information privacy, and family privacy (e.g., keeping home addresses confidential). Parents also reported approaches such as discussions and situational simulations to facilitate their children's comprehension and privacy management. Most parents adopted an "active but not invasive" strategy in educating their children about privacy. P03 (35-44, M) emphasized,

"*I try to be very active in my kid's life. And I have to be very active and not invasive at the same time.*" (P03, 35-44, M)

Parents indicated that they were only there when their children had privacy issues rather than monitoring them all the time. P05 (35-44, F) said,

"*I don't need to know everything about her, I don't need her to give me all the access. I only talk to her when I realize that it seems like something is wrong somewhere and I feel like I have to intervene.*" (P05, 35-44, F)

Children as Privacy Experts. Interestingly, when viewing privacy education at the family level, many children have also played a new role as privacy experts and took the responsibility to teach other family members about privacy.

We noticed the discrepancies between parents' impressions of their children's privacy awareness and children's actual knowledge level of privacy. Many children in our study demonstrated a strong sense of privacy and were able to leverage the knowledge they acquired from the Internet, their peers, and their hands-on experiences to guide their behaviors. For example, C02 (12-14, M) set complex passwords and frequently updated them. When using the Internet, many children also remained vigilant about data collection and sharing by social media companies and third parties, taking preventive measures to protect sensitive personal data, such as accounts, passwords, and browsing history. Because of that, many children shared privacy protection methods (particularly regarding online privacy) that they found useful with their family members, such as their parents and siblings. As C03 (12-14, M) said, he shared with his family the information about VPN protection obtained from a school club, emphasizing its application while using various apps or services.

Similar conversations also happened among siblings. Children were keen to share their privacy knowledge with their siblings to help them remain private online. For example, C03 (12-14, M) said,

"*I taught my sister to change the password every three months ..... She finds it stressful. She says, oh, nobody's trying to actually interact. So instead, I make her change the passwords every three months, as opposed to monthly, but I do mine. And now she's getting used to it.*" (C03, 12-14, M)

It should be noted that for the conversations among siblings, aside from discussing privacy protection, many siblings also engaged in conversations about evading their parents' control over their privacy. For instance, C01 (12-14, M) mentioned that he and his sibling often discussed how their parents, through parental controls, could monitor their tablet usage and how to escape from such monitoring. These kinds of interactions, on the one hand, demonstrated that children could become privacy experts and pass the knowledge to other family members, yet on the other hand, also showed the tension within the family surrounding privacy education and protection. We will further unpack this point in Section 4.2.1.

4.1.2 Privacy Education Was Often Carried Out through Open Conversations.

The second characteristic of family-based privacy education related to the role of open conversations - among the families we interviewed, having open conversations between parents and their children remained the primary and one key channel for communicating privacy. Most participants considered "open conversation" as an interaction that involved all family members to establish family norms regarding privacy, rather than answering a question with a "yes" or "no". Echoing Alghythee et al.'s work in which they characterized the conversation between parents and children when discussing privacy-related questions [3], our data also suggested that such interaction was often context-dependent, and adults outside of the family typically were not part of it.

Oftentimes, parents and children openly discussed their privacy experiences and concerns, then collaboratively learned about privacy as well as managed children's privacy. For example, P04 (35-44, M)'s partner discreetly installed a camera in their child's room. At the beginning, their child C04 (9-11, M) did not realize the existence of the camera. Then, before C04 found out about the camera, his parent decided to talk to him about it to understand his opinion. They discussed the situation and then reached a consensus that the camera was an invasion of the child's privacy, which promptly led to the camera's removal. In other cases, parents and children exchanged privacy knowledge through conversations. P01 (35-44, M) said,

"*My boy is frequently on social media. I always have conversations with him, whether it's online or offline. There's a limit to what you can share out there.*" (P01, 35-44, M))

As most parents reported, when their children were relatively young, they tended to set rules for their children to follow. As children got older, parents started to communicate with them and

guide them in understanding and managing privacy, such as discussing how to protect privacy, delineating permissible actions, outlining what was not allowed, enumerating potential negative outcomes, and providing examples. In this process, parents often expressed their privacy concerns towards their children and the rationale behind their decisions, while their children were able to voice their thoughts. Once an agreement was reached, both parents and children tended to have a better understanding of the expectations, including privacy expectations, within the family, which later became norms.

4.1.3 Privacy Education Often Happened in Specific Contexts. Another characteristic of family-based privacy education related to the fact that such education often happened in situ in specific contexts, as it often emphasized practicality and the resolution of specific concerns. In proactive privacy education, children primarily learned how to manage privacy issues. As C01 (12-14, M) said,

"*My dad always reminds me to ensure that our messages remain private and those secrets, even family secrets, should not be disclosed easily.*" (C01, 12-14, M)

To do this, parents frequently provided hands-on demonstrations of privacy protection features. For instance, P05 (35-44, F) shared an experience where she discovered her child texting a stranger. She initiated a conversation with her child, emphasizing the risks associated with compromising privacy and the potential consequences of texting to strangers. She shared,

"*I say you may think it's irrelevant, but it's very easy for an adult to read a minor a lot of times. Sometimes the other side through your answer, probably the other side can guess how old you are, but also can guess a lot of information about you.*" (P05, 35-44, F)

To further help her child understand the risks and potential consequences, she conducted a simulation with her child. She tried to chat with her child from the perspective of a stranger online and asked her for different types of information, then inferred her personal information based on the conversation. She referred to this experience as "in-depth privacy learning" which primarily occurred through direct conversations between parents and children following a privacy incident. When such an incident happened, parents were motivated to walk through the incident with their children while the children would also take the initiative to discuss it with their parents more openly and implement the suggested changes. However, P05 also emphasized the varied nature of privacy-related situations, necessitating a personalized approach to address each specific concern. Typically, she would provide general education to children and customize her engagement based on the specific nature of any arising problem issues.

Relatedly, many parents also mentioned the idea of integrating the discussion of privacy into their daily routine. For instance, P04 (35-44, M) mentioned incorporating privacy-related topics while escorting their child to school, and P06 (45-54, M) highlighted discussing relevant subjects during meal times with their children. They considered privacy education as a part of everyday general education for children. Therefore, when their children were young, instead of setting aside specific time for privacy education, they integrated certain rules into daily conversations. Additionally, many parents believed that privacy education should "*go hand in hand*" with other forms of education. For instance, P04 (35-44, M) mentioned teaching his son both respecting women and respecting privacy simultaneously.

4.1.4 Privacy Education Is a Continuous Process. Finally, unlike teaching privacy through other materials, family-based privacy education is a continuous process, which is further tailored to the distinct needs and developmental stages of children.

As we have seen in our data, parents commonly initiated privacy awareness and management with their children when they were young, starting with physical and spatial privacy (P01, 35-44, M; P04, 35-44, M; C07, 6-8, M). As children got older, their interaction with diverse people, technologies, and environments started to involve a deeper understanding of privacy. At this stage, parents often started to impart knowledge about online privacy, covering aspects like social media and passwords. As children became more mature, they would seek more personal space. They might start to engage in more sophisticated privacy behaviors, such as withholding their browsing history (C03, 12-14, M) or restricting parental access to their photos (C02, 12-14, M), etc. At this stage, privacy education would need to focus on increasing children's privacy literacy, as they need to learn how to independently manage their privacy while earning parental respect. At the same time, parents should understand the importance of respecting their children's boundaries and providing timely and appropriate assistance. As P03 (35-44, M) mentioned, when his child grew older, the timing of privacy education became critical,

"*I have to choose the right time. That's very, very important. And I need to have a vague idea of what I'm going to discuss with them.*" (P03, 35-44, M)

4.2 Challenges of Existing Family Privacy Education

Our data suggested that most families were able to engage in privacy education with their children. Yet, the outcomes often fell short. For example, P07 (35-44, F) told us that she had instructed the child not to share their family address, password, or other private information with anyone. However, when interviewing C07 (6-8, M), he shared their family address at the very beginning of the interview. Within the first ten minutes of the interview, C07 also disclosed the password to his iPad, which was his birthday [1]

Our data further suggested many challenges in current family-based privacy education practices. These challenges included tension among different family members, the complex and contextual nature of privacy, limited educational approaches, and a lack of educational support.

4.2.1 Tensions among Different Family Members. One prominent challenge related to the tensions among different family members, including crossing each other's boundary and overprotection causing surveillance concerns.

Crossing each other's boundary. At the early stage of childhood, when children lacked a comprehensive understanding of

[1]Authors' note: C07 provided the password voluntarily. In this case, we asked C07 not to share any sensitive information in the rest of the interview. We also removed the password from the recording.

privacy, they violated other family members' boundaries. For instance, C03 (12-14, M) mentioned that in his younger years, he used his father's phone to play games. His father, however, believed that "*he needs his own privacy wouldn't let me use his phone for gaming because he asked a lot of things or a couple of things he wants to protect*" and thus restricted the usage.

Similarly, parents also violated their children's privacy, especially as the children got to understand privacy and started to carry secrets they did not want to share with their parents. C06 (12-14, F) said,

"*I just like, don't want him to see like, stuff between my friend and I. It's not like there's anything bad, but I just like, want him to stay out of it.*" (C06, 12-14, F)

Overprotection may cause surveillance concerns. When it comes to privacy, the majority of our parent participants wanted to give their children maximum protection. However, such protection may result in invading their children's privacy, such as attempting to install cameras in children's rooms (P04, 35-44, M), asking for their passwords (P01, 35-44, M), and inspecting their conversations with friends (P06, 45-54, M). This type of invasion may encourage resistance from the children and prompt them to safeguard their privacy by withholding information and circumventing parental oversight. C02 (12-14, M) shared,

"*My parents do not recommend these movies for us but then I feel like yeah I'm old enough to get these. I'm 14. I can handle myself. So most times I don't allow my parents to have access to the kind of videos I watch on social media. I don't even give my parents my password FOR my Netflix accounts even though my dad subscribes on behalf of everyone.*" (C02, 12-14, M)

In fact, many children kept passwords and account information away from their parents (C01, 12-14, M; C05, 12-14, F). A few children maintained dual accounts, concealing one from their parents by using separate devices or timely logouts. P01 (35-44, M) shared about his second account,

"*My dad has parental control on my phone. So he sees most of the test. He knows about a on my smartphone. I have a second account only on my tablet because my dad does not know about my second account.*" (P01, 35-44, M))

Additionally, parents and children typically had different ways of handling their privacy considering the difference in their life stages and environments as well as their privacy preferences, resulting in potential conflicts. P04 (35-44, M) and P06 (45-54, M) both highlighted the different interpretations of privacy between parents and children, even though they respected each other's boundaries. P06 mentioned that his child had a broader understanding of privacy and a stricter approach to privacy protection and management compared to him. For instance, his child may consider many things as private while he did not share the same opinion.

4.2.2 Complex Contextual Nature of Privacy. Another challenge of family-based privacy education related to the contextual nature of privacy [68]. The intricate contexts associated with privacy problems in daily life posed significant challenges to effectively carrying out educational efforts. As P04 (35-44, M) said,

"*I feel (teaching) privacy is slightly more challenging because it's closely tied to his (child's) experiences in life.*" (P04, 35-44, M)

P04 further pointed out that one of key parameters in his child's life experiences was the evolving technologies. Unique privacy challenges emerged together with new technologies, requiring a continuous reassessment of educational strategies. Yet, many parents in our study did not have resources or ways to keep up with such requirements. Furthermore, children also had difficulties in discerning the appropriate privacy rules across different contexts. As such, existing privacy education approaches in families, such as family-based conversation, could not cover the breadth of possible privacy risk scenarios. For instance, common instructions such as "*do not disclose your home address to strangers*" would be challenging for children to implement in real life as children often struggled to identify "*strangers*" accurately.

4.2.3 Limited Educational Approaches. As mentioned in Section 4.1.2, family-based privacy education focused on open conversations. Yet, this conversational educational approach presents various challenges. Primarily, conversations, especially between parents and children, often led to emotional conflicts, indicating the need for diversified educational approaches. P02 (25-34, Non-Binary) highlighted that children may occasionally display strong resistance, causing frustration and impeding effective communication. They stated,

"*Issue you experience in education about privacy is, just being rebellious, initially.*" (P02, 25-34, Non-Binary)

Furthermore, the content of most educational conversations was typically monotonous, primarily focusing on privacy rules and potential negative consequences based on the given problem and context. Children in our study found this repetitive educational method tedious and unpleasant (judging by their tone during the interviews). Many parents shared similar concerns. P06 (45-54, M) said his observation,

"*As for the older child, basically she doesn't like this way, but she doesn't have a very strong frontal resistance. But the younger child has some signs of this, so I'm thinking about this too.*" (P06, 45-54, M)

4.2.4 Lack of In-Depth Knowledge among All Family Members. Another challenge discussed by our participants was that both parents and children currently lack adequate educational support to increase their privacy literacy. Among our participants, parents educated their children about privacy primarily based on their own educational backgrounds, life experiences, discussions with other parents, and some research through social media and the Internet. Yet, many parents (e.g., P03, 35-44, M; P08, 35-44, F) mentioned that they did not have sufficient knowledge to support more in-depth conversations nor guide their children towards more comprehensive privacy protection. P08 (35-44, F) said,

"*Maybe his (privacy) education is still a little poor because I know less about privacy.*" (P08, 35-44, F)

As a result, parents tended to seek resources and more information from social media and other online resources. P03 (35-44, M) shared,

"*Most of the time, I meet challenges in educating my children about privacy. I need to have a vague idea of what I'm going to discuss with them. That's why I do my research on various topics such as identity theft, social media, cyberbullying, and everything related to that, so I can have an in-depth understanding of what I want to discuss with them. In case they have questions, I will be able to answer their questions and put their concerns to rest.*" (P03, 35-44, M)

Unfortunately, these resources typically did not provide systematic privacy education to increase parents' privacy literacy. They also tended to be broadly about general privacy rules rather than detailed information that explicitly focused on privacy literacy. Consequentially, parents often found themselves lacking the necessary privacy knowledge to address their children's questions adequately and struggled to devise solutions when their children encountered privacy problems.

4.3 Family-based Learning Experiences in ILS

One of the main motivations of our study is to understand whether and how families utilized ILS (e.g., museums, science centers, libraries, historical sites, etc.) for family-based learning, which may potentially provide new possibilities for family-based privacy education. While all participating families engaged in privacy education, they struggled to foster robust privacy literacy to address privacy challenges effectively. Our findings indicated a widespread acknowledgment among both parents and children regarding the efficacy of ILS. Parents perceived ILS as a stimulant for their children's curiosity and creativity, resulting in "teachable moments" for more effective learning. For instance, P01 (35-44, M) said,

"*I feel like it ignited a major force in them. I feel like seeing does wonders. I feel like it is engineers, athletic engineers, creativeness, IT engineers creativity in your mind like they could go out there any future and become whatever they want.*" (P01, 35-44, M))

Similarly, children also showed a strong connection to ILS, finding them engaging and enlightening due to the diverse array of interactions they may offer. C05 (12-14, F) expressed,

"*And I feel like it's a great study spot and it's where one of the most productive places that I can be asked for museums and museums and like science center.*" (C05, 12-14, F)

Inspired by families' positive experiences in ILS, we further investigated the key characteristics from a family-based learning perspective and summarized four reasons why families may benefit from ILS, including 1) quality family times; 2) embodied experience; 3) exploratory and creative learning; and 4) long-lasting influence.

4.3.1 ILS Warranty Quality Family Time. All families in our study have visited some type of ILS before. As they discussed their experiences, we found that families, when visiting different ILS, often were able to spend quality time with the family members. For example, to enhance children's experiences when visiting ILS, parents often did some research about the places to get prepared (e.g., P04, 35-44, M). During the visit, parents and children often explored the place together. Throughout the visit, they might take photos (P02, 25-34, Non-Binary), interact with demonstrations and exhibits (e.g., P03, 35-44, M; P04, 35-44, M; P05, 35-44, F), and actively engage in discussions.

In these environments, family-based conversations were an essential part of the experience. Both parents and children could initiate conversations, and when that happened, it was often to stimulate their children's exploration and interest in various objects in the environment. Generally, parents initiated conversations by inquiring about their children's opinions on exhibits, models, or books, laying the foundation for further exploration. As C04 (9-11, M) said,

"*Sometimes my parents will go like, what did you learn? Like, something like that?*" (C04, 9-11, M)

Parents also helped their children explore other aspects (e.g., history) behind artworks (P02, 25-34, Non-Binary) or related the exhibit to everyday phenomena or stories for their children (P04, 35-44, M). For example, C05 (12-14, F) shared,

"*My mom will sometimes like, tell me oh, the motion of the tide or something? Or how seeds get transported from place to place? But yeah.*" (C05, 12-14, F)

From the children's perspective, they often shared novel experiences with their parents, seeking to gain more knowledge about these matters through ensuing discussions. P04 (35-44, M) provided an example in which his child was able to ask many questions related to the exhibits,

"*He would say, 'Dad, why is the electromagnetic situation like this? Why does static electricity make my hair stand up?' We would then discuss how static electricity transforms into attraction, and so on.*" (P04, 35-44, M)

At times, similar to the phenomenon we observed in Section 4.1.1, children also took on the role of teachers and proactively engaged in discussions with their parents. P04 (35-44, M) continued to give us an example in which his child became so obsessed with the exhibit in a local science center,

"*My child said 'Dad, I understand. Should I teach you this?'*" (P04, 35-44, M)

These examples and perspectives suggested that when visiting ILS, families were often able to spend quality family time together and have active and positive interactions among family members. Such quality time also enhanced children's learning appetite so that they would actively seek more knowledge. We believe that the quality time spent during families' visits to ILS as well as children's strong learning desires could offer an alternative approach to privacy education, which oftentimes was regarded as "tedious and boring" by our participants. We will further unpack this point in the discussion section.

4.3.2 Enriching Learning. Both parents and children in our study believed that ILS served as grounds for exploratory and creative learning experiences due to the interactive and embodied nature of ILS learning. The wide range of interaction modalities in ILS, such as interactive designs, exhibits, and experiments, not only provided alternative ways of learning new concepts but also encouraged learners, especially children, to independently delve into subjects, igniting their curiosity and fostering exploration. Many children expressed immense enjoyment in engaging in creative activities in ILS, such as painting, crafting, and workshops. At times, the interactivity embodied in different activities also encouraged children to think beyond the activities themselves. For example, C05 (12-14, F) mentioned her experience in a local museum and how the objects in the exhibit provided her with a new perspective,

"*There also like recreations of models, such as train cars, etc. That sort of made me think about it a little more and view it in a way I hadn't before about the Holocaust. So I think that applies to every sort of museum.*" (C05, 12-14, F)

Moreover, numerous ILS organized competitive events for visiting children, providing them with opportunities to earn awards

and fostering a sense of accomplishment, further encouraging continuing exploration. As C02 (12-14, M) shared her experience,

"*The most satisfying experience for me in these places was winning an award for the best night grader who ever used the museum. When you get rewarded for something you've done, it motivates you to strive for more and achieve greater things.*" (C02, 12-14, M)

4.3.3 Long-Lasting Influence in Life. Finally, our participants also reported that ILS played a pivotal and continuous role in shaping the long-term learning experiences within families beyond individual visits to ILS. For instance, after visits to various ILS, families tended to continue discussing their experiences, particularly triggered by scenarios related to the activities they experienced during their visits. P03 (35-44, M) described,

"*After the visit, we usually discuss things like 'What did you like most about this visit?' And it was during this time that we explored different cultures and went to see the dome... So we all had a thorough discussion about it ...*" (P03, 35-44, M)

Such long-lasting influence was embedded in everyday life and often occured seamlessly and naturally. For instance, as P06 (45-54, M) shared,

"*I occasionally chat with them, for example, the last time we saw this thing (at ILS)... When you're driving on the highway, you can explain to them why the road is curved, why it's not completely flat, and why there are speed limits.*" (P06, 45-54, M)

It should be noted that these discussions often occurred spontaneously whenever children showed curiosity about related subjects. As P02 (25-34, Non-Binary) confirmed,

"*Usually, this is a continuous process. Because it's quite inquisitive. You'd ask again. And I actually encourage that because it helps. With your learning as well.*" (P02, 25-34, Non-Binary)

In addition, many families expressed a tendency to revisit specific ILS, particularly museums, galleries, and science centers. These revisits would serve as opportunities for recurring discussions regarding their experiences. As P03 (35-44, M) expressed,

"*I have actually cultivated that nice habit in my kids to be very curious about historical things (by going historic museums).*" (P03, 35-44, M)

5 DISCUSSION

In this paper, we proposed the concept of *family-based privacy education in informal learning spaces* as a promising approach to enhancing children's learning of privacy and improving their privacy literacy. This is different from the mainstream children-centered privacy education in the literature and in practice. To further investigate the unique characteristics and challenges of *family-based privacy education* and explore the design opportunities for carrying out such education in *informal learning spaces (ILS)*, we conducted an interview study with 8 family groups to understand the current privacy education practices in their family and how they leveraged ILS as a way of learning. In this section, we reflect on the insights we gained in our interview and discuss why the proposed approach has the potential to transform the landscape of privacy education for children. We then discuss the design opportunities for designing interfaces to support family-based privacy education in ILS from four perspectives, i.e., design goals, educational content, engagement and interaction, and experience design. Also, we explore how these insights can inform future research and design about family-based privacy education in ILS.

5.1 Why Family-based Privacy Education May Work in ILS?

Our data suggested that family-based privacy education within ILS may serve as a bridge to fill gaps present in the current children-centered privacy education. ILS possess three key characteristics: warranty quality family time, enriching learning experiences, and ongoing influence. These aspects not only accentuate the existing strengths of family privacy education but also address its limitations.

As shown in Figure 2, the quality family time in ILS provides an opportunity for children to adequately and actively play their role in the learning process as well as engage in open conversation about privacy with their siblings and parents, which may further help mitigate the tension among different family members. For example, in Section 4.2.1, familial tensions pose a challenge for privacy education within family settings. Facilitating open communication and shared exploration among family members, as detailed in Section 4.3.1, can effectively mitigate these tensions.

Additionally, such interaction may extend beyond families' visits to ILS and continue to spark relevant conversations within the family. The long-term engagement further guaranteed that children would have the opportunity to continue discussing privacy and related topics with their parents in different contexts, which would be closer to the contextual nature of privacy [68]. Similarly, when privacy education happens in a specific context in ILS (e.g., an interactive exhibit that visualizes how data flows among different devices and entities in a smart home setting), it would spark several "teachable moments". For instance, in the example of an interactive exhibit that visualizes data flows within a smart home, when the children discover that some information is being sent to a mysterious third-party server, it is a "teachable moment" to educate them about the concept of "third-party tracking", "ad network", and other concepts. These teachable moments would provide specific scenarios for children to contextualize their learning, help them to understand the complex nature of privacy more easily, and at the same time, provide deeper knowledge that reveals the facts behind the observable phenomenon on the surface.

5.2 Design Opportunities of Interfaces to Support Family-based Privacy Education in ILS

Our empirical data hinted that children were taking active measures to protect their privacy, such as changing passwords regularly and safeguarding personal information. Yet, these methods may not be as effective as children may not do them correctly due to the lack of fundamental privacy knowledge, calling for more privacy education support. In this section, we discuss the design space from four perspectives, as detailed below.

5.2.1 Design Goals. Design goals refer to the high-level objectives that family-based privacy education interfaces should achieve to best leverage the unique advantages of ILS. We identified three main design goals as discussed below.

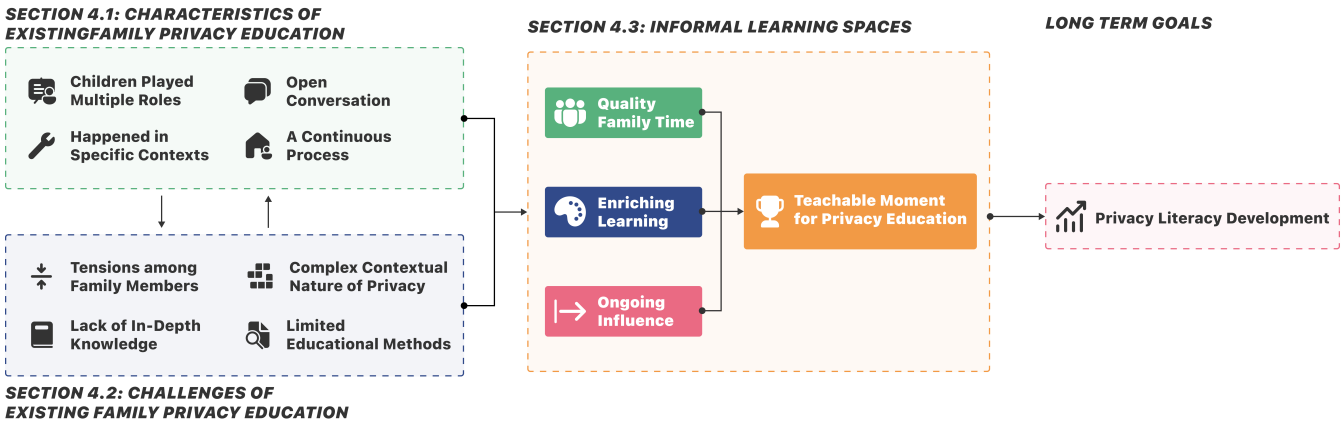

Figure 2: A mapping that illustrates why family-based privacy learning in informal learning spaces can be effective in mitigating the challenges in privacy education.

Goal 1: Family-Centered Learning. In Section 4.1.1, we emphasized that children learn about privacy from their family members (e.g., parents, siblings, etc.), aligning with previous research [11, 23, 24]. This is also a mutually beneficial process that could benefit all family members in terms of their understanding of privacy. As such, we argue that when designing privacy education interfaces in ILS, **we should focus on enhancing the experiences of the family groups rather than focusing on the needs of the children**. This family-centered approach in design has the potential to create more meaningful and relatable experiences for children and their families [16]. In certain cases (e.g., designing interfaces for young children), pivotal family members, such as parents, play a crucial role in building and reinforcing privacy literacy. They are also the first educators for their children who also impart essential privacy concepts in their day-to-day lives. Therefore, when designing family-based privacy education interfaces in ILS, it is also crucial to **pay particular attention to parents' involvement** to ensure they grasp the importance of privacy education, actively participate in the educational journey, and effectively advocate for privacy education.

Goal 2: Resolving the conflicts and tensions among family members. As described in Section 4.2.1, the tensions among family members were a significant challenge when discussing privacy-related issues within the family. These tensions may result in conflicts and mistrust between children and parents, impeding open communication within the family regarding privacy. Furthermore, adults' respect for children's privacy is critical to developing children's privacy literacy [48], yet the privacy norms within families were not always clear. On the other hand, both parents and children perceived ILS as a relaxing environment that could facilitate meaningful communication. Hence, privacy education interfaces in ILS should also aim to **foster a safe and flexible environment for family members to expose potential privacy-related conflicts and tensions, have open conversations about those conflicts, and establish privacy norms in the family.**

Goal 3: Cultivation of Privacy Literacy. Prior research advocates promoting one's privacy literacy instead of the mere instruction of privacy regulations [40, 60]. Our data suggested that some parents' strategies to protect their children's privacy would involve setting different rules for children of different age groups. Yet, setting privacy rules was considered a less effective way of managing privacy [48].

On the contrary, privacy literacy is a form of critical thinking [94], where learners gradually apply their skills from simple to complex instances. Ultimately, they should employ their knowledge and skills in real-world scenarios [48, 49]. In Section 4.3.2, both children and parents find ILS conducive to fostering expansive learning and nurturing their inquisitiveness, suggesting the unique possibility of ILS in improving children's privacy literacy. Consequently, we believe that privacy education interfaces should treat **the promotion of privacy literacy as a key objective** within ILS.

5.2.2 Educational Content. Educational content refers to the specific content that family-based privacy education interfaces should include. We summarized the following two critical types of content based on the challenges we identified in Section 4.2 as well as the dynamics in families.

Content 1: Foundational Privacy Principles and Concepts. Section 4.2.2 demonstrated that complex contexts remain an important challenge in family-based privacy education. Parents found it challenging to encompass all privacy contexts for their children. Such complexity also made it difficult for parents to provide deep insights and rationales about privacy-related phenomena and suggest nuanced approaches in diverse contexts. Yet, most existing privacy education materials opt to focus on practical solutions and rules rather than introducing fundamental concepts of privacy. We believe that family-based privacy education interfaces should **enable systematic privacy learning with a specific focus on fundamental privacy concepts, such as consent, privacy norms, and information flow.** For example, it is vital for parents to connect rules to norms and discuss rules in terms of contextually appropriate information flows [49]. The interactive and engaging environment in ILS also makes it easier to learn about such fundamental concepts.

Education content should also connect these principles to real-life contexts. For instance, it should expound on how the principle of consent guides the sharing of personal information online or

how data security principles underpin the protection of sensitive data on digital platforms. Such connections would allow learners to relate privacy concepts to their everyday experiences, enhancing engagement and impact in the learning process. This educational content serves to bolster privacy awareness and literacy, particularly among children and parents. A sound grasp of these core principles empowers individuals, especially children, to make informed decisions regarding their privacy across a spectrum of life situations.

Content 2: Contextual Practice Skills. In Section 4.1.3, we outlined that current family privacy education typically occurs in specific contexts, focusing on imparting practical skills. This aligns with Kumar et al.'s privacy education goal based on the contextual integrity framework: privacy education should aim to enable individuals to make privacy-related decisions that genuinely benefit them, rather than merely instructing adherence to privacy rules [48, 49].

Therefore, family-based privacy education interfaces should **provide content related to families' varying privacy needs and their practices in different contexts.** ILS could provide unique possibilities to customize the content, e.g., leveraging end-user programming techniques to learn about families' actual practices; creating reusable modules that can be easily re-grouped to form new contexts (accordingly to the Theory of Contextual Integrity [68]). Additionally, ILS can present hands-on experiences and real-life applications using different methods, such as scenario simulations, role-playing, and interactive devices. For instance, involving children and parents in privacy-related decision-making within a specific context allows them to learn privacy norms in the context. An example is to understand the privacy policies of online services or apps before using them, and then comprehend data collection, usage, and sharing mechanisms. Incorporating practical skills into educational content directly assists individuals in making informed privacy-related decisions in their daily lives, thereby enhancing their privacy literacy.

5.2.3 Engagement and Interaction. Engagement and interaction refer to how family-based privacy education interfaces engage their users (i.e., family groups) and what types of interaction modality should and should not be allowed.

Promote Family Interaction. In ILS, we found two factors that may influence children's learning outcomes, including whether there are tensions among different family members and whether parents can learn with their children in a conducive environment. We believed that **ILS should encourage family members to learn together, reinforcing their comprehension of privacy topics through discussions.** There are various methods to boost family interactions in ILS as outlined in Section 2.3.2. One effective approach is to promote family-based learning by directing joint attention to an object during their visit and creating interactive activities or games that engage all family members. This can also be facilitated by leveraging the patterns in family-based conversations [3]. These activities can include privacy-related topics that deepen family members' understanding of privacy issues and lead to productive discussions.

Multiple ways to achieve interactivity. Interactive learning offers a great way to enhance privacy education in ILS. As explained in Section 4.3.2, ILS provides hands-on and enriched learning experiences for parents and their children. Given the nature of ILS, privacy education in such contexts should **leverage the unique interaction modality in ILS and be creative on the format of privacy education.** For example, tangible objects can be used to enable hands-on interactions (e.g., the data flow among smart home devices can be visualized as light signals through an LED light stripe), which was proven to be effective in achieving this immersive and enriching learning experience [64, 85]. Displaying privacy-related principles through interactive exhibits and using AR or VR for an immersive experience may also make the learning process more engaging. Additionally, integrating real-world applications and incorporating gamification in those applications can also simulate privacy-related scenarios effectively [18].

5.2.4 Experience Design. Experience design refers to the type of experiences that family-based privacy education interfaces in ILS should support.

Children-Friendly Education Materials. Privacy education in ILS should **start with topics that are familiar and relevant to children,** such as personal privacy regarding their bodies, family address, SSN number, etc. Such education may also cover topics directly linked to children's lives, such as the safe usage of social media and how to manage personal information. Educational materials should **employ clear, simple, and easily comprehensible language in presentations** rather than complex or specialized terminologies, and **include content that is appropriate for different age groups within the family.** Our findings support the latter point, e.g., C06 pointed out that certain museum exhibits or activities were too simplistic for her, whereas C08 found some exhibits unattractive for his younger brother.

Parents as Learners and Facilitators. As Section 4.2.4 described, it is difficult for some parents to provide effective privacy help to their children due to their own limited privacy knowledge and privacy educational materials. Given the lack of educational support, it is important to **provide parents with the necessary knowledge and guidelines when providing privacy education in ILS.** When visiting ILS, privacy education should promote learning and interaction between children and parents, which may also help many adults develop privacy literacy. Ideally, after visiting, children can receive continuous privacy learning support from their parents in their daily lives. These resources and guidance take various forms. For instance, informative signs with prompts and detailed explanations can be employed, aiding parents in explaining concepts or engaging in discussions with their children. Additionally, parents can receive additional resources or reading materials in advance that outline educational objectives, suggested activities, and strategies for involving children in privacy education within specific ILS. Offering privacy courses or take-home instructional materials for parents can further empower them to grasp privacy knowledge and skills, allowing them to provide sustained assistance to their children in their daily lives.

5.3 Method Reflection

5.3.1 Approaches to Interview Parent-Child Pairs. In this study, inspired by the work of McReynold et al.'s work [61], we deliberately

chose to interview children and parents from the same family separately. Acknowledging other possible ways to conduct research in similar settings, in this section, we discuss our reflection on the interview settings and process.

We believed that by interviewing children and parents separately, we would gain a comprehensive understanding of parents' and children's thoughts and experiences without causing potential tension and conflict within family settings. Furthermore, even though we asked the participants to determine the interview order, we observed that interviewing parents first, particularly when dealing with young children, had an extra benefit - parents could typically provide researchers with foundational knowledge about the family dynamics and children, facilitating smoother interactions during the subsequent interviews with the children. This was particularly important due to the nature barriers when conducting studies with children.

Aside from this approach, literature has also suggested two alternative approaches to interviewing parent-child pairs. One option is to interview only one individual (either the child or the parent) from each family. This approach, advocated in previous studies[21, 25], respects teenagers' right to privacy, particularly if they prefer not to share their experiences with their parents. This method helps avoid potential conflicts or embarrassment among family members. While effective for capturing sensitive experiences and thoughts, it may overlook paradoxes in family dynamics. For instance, in our study, P08 instructed her child not to share personal information, yet C08 disclosed it freely. Interviewing only one member of the pair would miss this contradiction.

In the privacy literature, researchers have also used other approaches to interview family groups, such as interviewing parents and children together [35, 79, 88]. It should be noted that each approach has its own unique pros and cons, yet we urge researchers to pay particular attention to the possible ethical issues that may arise in this process. We briefly discuss them below.

5.3.2 Strategies for Safeguarding Children's Privacy During Interviews. As shown in our research, children may disclose sensitive personal information (e.g., passwords) during the interview, making it critical to protect their data privacy and safety during and after the study. We made the following suggestions to ensure ethical conduct during children-related research.

Firstly, before the study, all research team members should go through ethical training on conducting research with children, typically provided by child welfare professionals. In sensitive research areas, such as research on sexual harassment or cyberbullying, researchers should consider having child welfare professionals onsite throughout the interview process to assist the research.

Additionally, establishing clear guidelines for handling sensitive information disclosures before the study is crucial. These guidelines should include the principles to handle accidental information personal information disclosure (e.g., remove such information from recordings or transcriptions) as well as measures to prevent similar disclosures in the remaining studies (e.g., constant reminders). It is worth noting that when communicating with children regarding privacy-related matters, the languages and terms should be tailored towards children's privacy mental models to ensure their understanding and compliance. In our study, we utilized terms such as locks, personal rooms, and special boxes from previous research [69] to familiarize children with the concept of privacy.

5.4 Future Work

In future research, we aim to actively engage with family groups in co-design activities to obtain design implements for privacy-related educational devices within informal learning spaces. Additionally, we plan to enhance diversity by incorporating more family groups with different backgrounds and collaborating with more stakeholders, such as educators and personnel from diverse informal learning spaces. We also plan to extend our research with additional scenarios, such as the sharing of electronic devices among siblings, inter-generational interactions involving grandparents, and the use of additional technologies such as IoT and wearables. This broader inclusion will provide richer insights into the varied experiences and needs of families in different contexts.

Furthermore, we intend to design and implement interventions based on our findings, with a commitment to an iterative process to continually refine and improve the effectiveness of these interventions. For example, families could work as a team in an interactive exhibition in which they fight against "privacy monsters" by dealing with various privacy-related problems. They will interact with the interface, leveraging tangible devices or AR/VR equipment to immerse themselves in a lifelike experience. This approach may contribute to our goal of identifying "teachable moments" and ensures a dynamic and responsive strategy in addressing the complex challenges of privacy education within family settings and informal learning spaces.

6 CONCLUSION

Faced with increasing privacy risks for children and constraints of existing privacy education, we introduced a **family-based privacy education approach in informal learning spaces**. An interview study involving eight families confirmed the viability of this approach in understanding the characteristics and challenges of current family privacy education, as well as how families utilize informal learning spaces for learning. In this paper, our findings offered design opportunities from design goals, educational content, engagement, and interaction, as well as experience design, thereby enriching the landscape of future research on family-based privacy education in ILS.

7 ACKNOWLEDGEMENT

We thank the anonymous reviewers for the constructive feedback. This work is in part supported by the National Science Foundation Grant 2341187 and 2328183, a Meta Research Award, and a Google Research Award.

REFERENCES

[1] Devon Adams, Alseny Bah, Catherine Barwulor, Nureli Musaby, Kadeem Pitkin, and Elissa M. Redmiles. 2018. Ethics Emerging: the Story of Privacy and Security Perceptions in Virtual Reality. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 427–442. https://www.usenix.org/conference/soups2018/presentation/adams

[2] Laila Robiatul Adawiah and Yeni Rachmawati. 2021. Parenting Program to Protect Children's Privacy: The Phenomenon of Sharenting Children on social media. *Jurnal Pendidikan Usia Dini* 15, 1 (April 2021), 162–180. https://doi.org/10.21009/JPUD.151.09 Number: 1.

[3] Kenan Kamel A Alghythee, Adel Hrncic, Karthik Singh, 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 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA,) *(CHI'24)*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3613904.3641962

[4] Khalid Alkhattabi, Ahmed Alshehri, and Chuan Yue. 2020. Security and Privacy Analysis of Android Family Locator Apps. In *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies (SACMAT '20)*. Association for Computing Machinery, New York, NY, USA, 47–58. https://doi.org/10.1145/3381991.3395612

[5] Sue Allen. 2004. Designs for learning: Studying science museum exhibits that do more than entertain. *Science Education* 88, S1 (2004), S17–S33. https://doi.org/10.1002/sce.20016 _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/sce.20016.

[6] Tawfiq Ammari and Sarita Schoenebeck. 2015. Understanding and Supporting Fathers and Fatherhood on Social Media Sites. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. Association for Computing Machinery, New York, NY, USA, 1905–1914. https://doi.org/10.1145/2702123.2702205

[7] Mary Jean Amon, Nika Kartvelishvili, Bennett I. Bertenthal, Kurt Hugenberg, and Apu Kapadia. 2022. Sharenting and Children's Privacy in the United States: Parenting Style, Practices, and Perspectives on Sharing Young Children's Photos on Social Media. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW1 (March 2022), 1–30. https://doi.org/10.1145/3512963

[8] Lucija Andre, Tracy Durksen, and Monique L. Volman. 2017. Museums as avenues of learning for children: a decade of research. *Learning Environments Research* 20, 1 (April 2017), 47–76. https://doi.org/10.1007/s10984-016-9222-9

[9] David Barnard-Wills and Debi Ashenden. 2015. Playing with Privacy: Games for Education and Communication in the Politics of Online Privacy. *Political Studies* 63, 1 (March 2015), 142–160. https://doi.org/10.1111/1467-9248.12049 Publisher: SAGE Publications Ltd.

[10] Mitchell K. Bartholomew, Sarah J. Schoppe-Sullivan, Michael Glassman, Claire M. Kamp Dush, and Jason M. Sullivan. 2012. New Parents' Facebook Use at the Transition to Parenthood. *Family Relations* 61, 3 (2012), 455–469. https://doi.org/10.1111/j.1741-3729.2012.00708.x _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1741-3729.2012.00708.x.

[11] Joke Bauwens, Katleen Gabriels, and Lien Mostmans. 2020. Navigating onlife privacy: A family environment perspective on children's moral principles. *Media and Communication* 8, 4 (2020), 185–196.

[12] Leslie Bedford. 2014. *The Art of Museum Exhibitions: How Story and Imagination Create Aesthetic Experiences* (1st ed ed.). Routledge, Walnut Creek, California.

[13] Elham Beheshti, David Kim, Gabrielle Ecanow, and Michael S. Horn. 2017. Looking Inside the Wires: Understanding Museum Visitor Learning with an Augmented Circuit Exhibit. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Association for Computing Machinery, New York, NY, USA, 1583–1594. https://doi.org/10.1145/3025453.3025479

[14] Nora Benjamin, Catherine A. Haden, and Erin Wilkerson. 2010. Enhancing building, conversation, and learning through caregiver–child interactions in a children's museum. *Developmental Psychology* 46 (2010), 502–515. https://doi.org/10.1037/a0017822

[15] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (Jan. 2006), 77–101. https://doi.org/10.1191/1478088706qp063oa Publisher: Routledge _eprint: https://www.tandfonline.com/doi/pdf/10.1191/1478088706qp063oa.

[16] Bengisu Cagiltay. 2023. Designing for In-Home Long-Term Family-Robot Interactions: Family Preferences, Connection-Making, and Privacy. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA '23)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3544549.3577035

[17] Maureen A. Callanan, Cristine H. Legare, David M. Sobel, Garrett J. Jaeger, Susan Letourneau, Sam R. McHugh, Aiyana Willard, Aurora Brinkman, Zoe Finiasz, Erika Rubio, Adrienne Barnett, Robin Gose, Jennifer L. Martin, Robin Meisner, and Janella Watson. 2020. Exploration, Explanation, and Parent–Child Interaction in Museums. *Monographs of the Society for Research in Child Development* 85, 1 (2020), 7–137. https://doi.org/10.1111/mono.12412

[18] Vanessa Cesário, Daniela Petrelli, and Valentina Nisi. 2020. Teenage Visitor Experience: Classification of Behavioral Dynamics in Museums. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376334

[19] Mauro Cherubini, Kavous Salehzadeh Niksirat, Marc-Olivier Boldi, Henri Keopraseuth, Jose M. Such, and Kévin Huguenin. 2021. When Forcing Collaboration Is the Most Sensible Choice: Desirability of Precautionary and Dissuasive Mechanisms to Manage Multiparty Privacy Conflicts. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW1 (April 2021), 53:1–53:36. https://doi.org/10.1145/3449127

[20] Malinda J. Colwell, Kimberly Corson, Anuradha Sastry, and Holly Wright. 2016. Secret keepers: children's theory of mind and their conception of secrecy. *Early Child Development and Care* 186, 3 (March 2016), 369–381. https://doi.org/10.1080/03004430.2015.1031657 Publisher: Routledge _eprint: https://doi.org/10.1080/03004430.2015.1031657.

[21] Lorrie Faith Cranor, Adam L. Durity, Abigail Marsh, and Blase Ur. 2014. Parents' and Teens' Perspectives on Privacy In a Technology-Filled World. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, Menlo Park, CA, 19–35. https://www.usenix.org/conference/soups2014/proceedings/presentation/cranor

[22] Kevin Crowley, Maureen A. Callanan, Harriet R. Tenenbaum, and Elizabeth Allen. 2001. Parents Explain More Often to Boys Than to Girls During Shared Scientific Thinking. *Psychological Science* 12, 3 (May 2001), 258–261. https://doi.org/10.1111/1467-9280.00347 Publisher: SAGE Publications Inc.

[23] Katie Davis and Carrie James. 2013. Tweens' conceptions of privacy online: Implications for educators. *Learning, Media and Technology* 38, 1 (2013), 4–25.

[24] 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.

[25] Elmira Deldari, Diana Freed, Julio Poveda, and Yaxing Yao. 2023. An Investigation of Teenager Experiences in Social Virtual Reality from Teenagers', Parents', and Bystanders' Perspectives. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. USENIX Association, Anaheim, CA, 1–17. https://www.usenix.org/conference/soups2023/presentation/deldari

[26] John Dempsey, Gavin Sim, Brendan Cassidy, and Vinh-Thong Ta. 2022. Children designing privacy warnings: Informing a set of design guidelines. *International Journal of Child-Computer Interaction* 31 (2022), 100446. https://doi.org/10.1016/j.ijcci.2021.100446

[27] Tamara Denning, Cynthia Matuszek, Karl Koscher, Joshua R. Smith, and Tadayoshi Kohno. 2009. A spotlight on security and privacy risks with future household robots: attacks and lessons. In *Proceedings of the 11th international conference on Ubiquitous computing (UbiComp '09)*. Association for Computing Machinery, New York, NY, USA, 105–114. https://doi.org/10.1145/1620545.1620564

[28] Stefania Druga, Fee Lia Christoph, and Amy J Ko. 2022. Family as a Third Space for AI Literacies: How do children and parents learn about AI together?. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (, New Orleans, LA, USA,) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 225, 17 pages. https://doi.org/10.1145/3491102.3502031

[29] Serge Egelman, Julia Bernd, Gerald Friedland, and Dan Garcia. 2016. The Teaching Privacy Curriculum. In *Proceedings of the 47th ACM Technical Symposium on Computing Science Education (SIGCSE '16)*. Association for Computing Machinery, New York, NY, USA, 591–596. https://doi.org/10.1145/2839509.2844619

[30] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, Glasgow Scotland Uk, 1–12. https://doi.org/10.1145/3290605.3300764

[31] John H. Falk and Lynn D. Dierking. 2000. *Learning from museums: visitor experiences and the making of meaning*. AltaMira Press, Walnut Creek, CA. OCLC: 43384923.

[32] Francisco Erivaldo Fernandes, Guanci Yang, Ha Manh Do, and Weihua Sheng. 2016. Detection of Privacy-Sensitive Situations for Social Robots in Smart Homes. In *2016 IEEE International Conference on Automation Science and Engineering (CASE)*. IEEE Press, Fort Worth, TX, USA, 727–732. https://doi.org/10.1109/COASE.2016.7743474

[33] Alexa K Fox and Mariea Grubbs Hoy. 2019. Smart devices, smart decisions? Implications of parents' sharenting for children's online privacy: An investigation of mothers. *Journal of Public Policy & Marketing* 38, 4 (2019), 414–432.

[34] Helen L. Gallagher and Christopher D. Frith. 2003. Functional imaging of 'theory of mind'. *Trends in Cognitive Sciences* 7, 2 (Feb. 2003), 77–83. https://doi.org/10.1016/s1364-6613(02)00025-6

[35] Radhika Garg and Subhasree Sengupta. 2020. He Is Just Like Me: A Study of the Long-Term Use of Smart Speakers by Parents and Children. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 4, 1, Article 11 (mar 2020), 24 pages. https://doi.org/10.1145/3381002

[36] 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 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376747

[37] Joshua P. Gutwill and Sue Allen. 2010. Facilitating family group inquiry at science museum exhibits. *Science Education* 94, 4 (2010), 710–742. https://doi.org/10.1002/sce.20387

[38] Catherine A. Haden. 2010. Talking About Science in Museums. *Child Development Perspectives* 4, 1 (2010), 62–67. https://doi.org/10.1111/j.1750-8606.2009.00119.x _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1750-8606.2009.00119.x.

[39] Christian Heath, Dirk Vom Lehn, and Jonathan Osborne. 2005. Interaction and interactives: collaboration and participation with computer-based exhibits. *Public Understanding of Science* 14, 1 (Jan. 2005), 91–101. https://doi.org/10.

1177/0963662505047343 Publisher: SAGE Publications Ltd.
[40] Velislava Hillman. 2022. Data privacy literacy as a subversive instrument to datafication. *International Journal of Communication* 16 (2022), 22.
[41] Alexis Hiniker, Sarita Y. Schoenebeck, and Julie A. Kientz. 2016. Not at the Dinner Table: Parents' and Children's Perspectives on Family Technology Rules. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16)*. Association for Computing Machinery, New York, NY, USA, 1376–1389. https://doi.org/10.1145/2818048.2819940
[42] Michael S. Horn, Erin Treacy Solovey, and Robert J. K. Jacob. 2008. Tangible programming and informal science learning: making TUIs work for museums. In *Proceedings of the 7th international conference on Interaction design and children (IDC '08)*. Association for Computing Machinery, New York, NY, USA, 194–201. https://doi.org/10.1145/1463689.1463756
[43] Mathias Humbert, Benjamin Trubert, and Kévin Huguenin. 2019. A Survey on Interdependent Privacy. *ACM Comput. Surv.* 52, 6 (Oct. 2019), 122:1–122:40. https://doi.org/10.1145/3360498
[44] Mikkel S. Jørgensen, Frederik K. Nissen, Jeni Paay, Jesper Kjeldskov, and Mikael B. Skov. 2016. Monitoring children's physical activity and sleep: a study of surveillance and information disclosure. In *Proceedings of the 28th Australian Conference on Computer-Human Interaction* (Launceston, Tasmania, Australia) *(OzCHI '16)*. Association for Computing Machinery, New York, NY, USA, 50–58. https://doi.org/10.1145/3010915.3010936
[45] Lee Kimche. 1978. Science Centers: A Potential for Learning. *Science* 199, 4326 (Jan. 1978), 270–273. https://doi.org/10.1126/science.619454 Publisher: American Association for the Advancement of Science.
[46] Priya Kumar and Sarita Schoenebeck. 2015. The Modern Day Baby Book: Enacting Good Mothering and Stewarding Privacy on Facebook. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '15)*. Association for Computing Machinery, New York, NY, USA, 1302–1312. https://doi.org/10.1145/2675133.2675149
[47] 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* (Trondheim, Norway) *(IDC '18)*. Association for Computing Machinery, New York, NY, USA, 67–79. https://doi.org/10.1145/3202185.3202735
[48] 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 (2022), 445–461.
[49] 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 (2020), 175–184.
[50] Anastasia Kuzminykh and Edward Lank. 2019. How Much Is Too Much? Understanding the Information Needs of Parents of Young Children. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 3, 2 (June 2019), 52:1–52:21. https://doi.org/10.1145/3328923
[51] Anne M. Land-Zandstra, Kelly Hoefakker, and Welmoet Damsma. 2020. Reasoning about Objects in a Natural History Museum: The Effect of Complexity of Questions on Object Labels. *Visitor Studies* 23, 2 (July 2020), 218–236. https://doi.org/10.1080/10645578.2020.1781485 Publisher: Routledge _eprint: https://doi.org/10.1080/10645578.2020.1781485.
[52] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (Nov. 2018), 102:1–102:31. https://doi.org/10.1145/3274371
[53] Min Kyung Lee, Karen P. Tang, Jodi Forlizzi, and Sara Kiesler. 2011. Understanding users' perception of privacy in human-robot interaction. In *Proceedings of the 6th international conference on Human-robot interaction (HRI '11)*. Association for Computing Machinery, New York, NY, USA, 181–182. https://doi.org/10.1145/1957656.1957721
[54] Merike Lipu and Andra Siibak. 2019. 'Take it down!': Estonian parents' and pre-teens' opinions and experiences with sharenting. *Media International Australia* 170, 1 (Feb. 2019), 57–67. https://doi.org/10.1177/1329878X19828366 Publisher: SAGE Publications Ltd.
[55] Duri Long, Takeria Blunt, and Brian Magerko. 2021. Co-Designing AI Literacy Exhibits for Informal Learning Spaces. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (Oct. 2021), 293:1–293:35. https://doi.org/10.1145/3476034
[56] Duri Long, Tom McKlin, Anna Weisling, William Martin, Steven Blough, Katlyn Voravong, and Brian Magerko. 2020. Out of tune: discord and learning in a music programming museum exhibit. In *Proceedings of the Interaction Design and Children Conference (IDC '20)*. Association for Computing Machinery, New York, NY, USA, 75–86. https://doi.org/10.1145/3392063.3394430
[57] Duri Long, Anthony Teachey, and Brian Magerko. 2022. Family Learning Talk in AI Literacy Learning Activities. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)*. Association for Computing Machinery, New York, NY, USA, 1–20. https://doi.org/10.1145/3491102.3502091
[58] Leilah Lyons, Brian Slattery, Priscilla Jimenez, Brenda Lopez, and Tom Moher. 2012. Don't forget about the sweat: effortful embodied interaction in support of learning. In *Proceedings of the Sixth International Conference on Tangible, Embedded and Embodied Interaction (TEI '12)*. Association for Computing Machinery, New York, NY, USA, 77–84. https://doi.org/10.1145/2148131.2148149
[59] Delfina Malandrino, Andrea Petta, Vittorio Scarano, Luigi Serra, Raffaele Spinelli, and Balachander Krishnamurthy. 2013. Privacy Awareness about Information Leakage: Who Knows What about Me?. In *Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society* (Berlin, Germany) *(WPES '13)*. Association for Computing Machinery, New York, NY, USA, 279–284. https://doi.org/10.1145/2517840.2517868
[60] 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 (TOPS)* 24, 4 (2021), 1–37.
[61] 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*. ACM, Denver Colorado USA, 5197–5207. https://doi.org/10.1145/3025453.3025735
[62] Tehila Minkus, Kelvin Liu, and Keith W. Ross. 2015. Children Seen But Not Heard: When Parents Compromise Children's Online Privacy. In *Proceedings of the 24th International Conference on World Wide Web* (Florence, Italy) *(WWW '15)*. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 776–786. https://doi.org/10.1145/2736277.2741124
[63] Ann Mintz. 2005. Science, society and science centres. *Historia, Ciencias, Saude–Manguinhos* 12, Suppl (2005), 267–280. https://doi.org/10.1590/s0104-59702005000400013
[64] Joan Mora-Guiard and Narcis Pares. 2014. "Child as the measure of all things": the body as a referent in designing a museum exhibit to understand the nanoscale. In *Proceedings of the 2014 conference on Interaction design and children (IDC '14)*. Association for Computing Machinery, New York, NY, USA, 27–36. https://doi.org/10.1145/2593968.2593985
[65] Meredith Ringel Morris. 2014. Social networking site use by mothers of young children. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing (CSCW '14)*. Association for Computing Machinery, New York, NY, USA, 1272–1282. https://doi.org/10.1145/2531602.2531603
[66] Carol Moser, Tianying Chen, and Sarita Y. Schoenebeck. 2017. Parents? and Children?s Preferences about Parents Sharing about Children on Social Media. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Association for Computing Machinery, New York, NY, USA, 5221–5225. https://doi.org/10.1145/3025453.3025587
[67] Rita Müller. 2013. Museums designing for the future: some perspectives confronting German technical and industrial museums in the twenty-first century. *International Journal of Heritage Studies* 19, 5 (July 2013), 511–528. https://doi.org/10.1080/13527258.2011.651736
[68] Helen Nissenbaum. 2004. Privacy as Contextual Integrity. *Washington Law Review* 79, 1 (Feb. 2004), 119. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10
[69] 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
[70] Luci Pangrazio and Neil Selwyn. 2017. 'My Data, My Bad ...': Young People's Personal Data Understandings and (Counter)Practices. In *Proceedings of the 8th International Conference on Social Media & Society (#SMSociety17)*. Association for Computing Machinery, New York, NY, USA, 1–5. https://doi.org/10.1145/3097286.3097338
[71] Farzana Quayyum. 2020. Cyber security education for children through gamification: research plan and perspectives. In *Proceedings of the 2020 ACM Interaction Design and Children Conference: Extended Abstracts (IDC '20)*. Association for Computing Machinery, New York, NY, USA, 9–13. https://doi.org/10.1145/3397617.3398030
[72] Kate Raynes-Goldie and Matthew Allen. 2014. Gaming Privacy: a Canadian case study of a children's co-created privacy literacy game. *Surveillance & Society* 12, 3 (June 2014), 414–426. https://doi.org/10.24908/ss.v12i3.4958
[73] Jake Reichel, Fleming Peck, Mikako Inaba, Bisrat Moges, Brahmnoor Singh Chawla, and Marshini Chetty. 2020. 'I have too much respect for my elders': Understanding South African Mobile Users' Perceptions of Privacy and Current Behaviors on Facebook and WhatsApp. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Boston, MA, USA, 1949–1966. https://www.usenix.org/conference/usenixsecurity20/presentation/reichel
[74] Jennifer C. Rigney and Maureen A. Callanan. 2011. Patterns in parent–child conversations about animals at a marine science center. *Cognitive Development* 26, 2 (April 2011), 155–171. https://doi.org/10.1016/j.cogdev.2010.12.002
[75] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth

Churchill. 2018. "Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 127–142. https://www.usenix.org/conference/soups2018/presentation/sambasivan

[76] Irit Sasson. 2014. The role of informal science centers in science education: attitudes, skills, and self-efficacy. *JOTSE: Journal of Technology and Science Education* 4, 3 (Sept. 2014), 167–179. https://upcommons.upc.edu/handle/2099/16277 Accepted: 2015-04-07T11:06:35Z Publisher: OmniaScience.

[77] Marie-Monique Schaper, Maria Santos, Laura Malinverni, and Narcis Pares. 2017. Towards the Design of a Virtual Heritage Experience based on the World-as-Support Interaction Paradigm. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '17)*. Association for Computing Machinery, New York, NY, USA, 2034–2041. https://doi.org/10.1145/3027063.3053089

[78] Guy Schofield, Gareth Beale, Nicole Beale, Martin Fell, Dawn Hadley, Jonathan Hook, Damian Murphy, Julian Richards, and Lewis Thresh. 2018. Viking VR: Designing a Virtual Reality Experience for a Museum. In *Proceedings of the 2018 Designing Interactive Systems Conference (DIS '18)*. Association for Computing Machinery, New York, NY, USA, 805–815. https://doi.org/10.1145/3196709.3196714

[79] G. Segre, R. Campi, F. Scarpellini, A. Clavenna, M. Zanetti, M. Cartabia, and M. Bonati. 2021. Interviewing children: the impact of the COVID-19 quarantine on children's perceived psychological distress and changes in routine. *BMC Pediatrics* 21, 1 (May 2021), 231. https://doi.org/10.1186/s12887-021-02704-1

[80] Jack P. Shonkoff and Deborah A. Phillips. 2000. *From Neurons to Neighborhoods: The Science of Early Childhood Development*. National Academies Press (US), Washington (DC). http://www.ncbi.nlm.nih.gov/books/NBK225557/

[81] Stacey B Steinberg. 2016. Sharenting: Children's privacy in the age of social media. *Emory LJ* 66 (2016), 839.

[82] 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

[83] Andrew A. Tawfik, Jessica Gatewood, Laura Armstrong, and Craig E. Shepherd. 2023. Informal Learning in United States Libraries: A Systematic Review. *TechTrends* 67, 3 (May 2023), 550–560. https://doi.org/10.1007/s11528-022-00811-z

[84] Harriet R. Tenenbaum and Campbell Leaper. 2003. Parent-child conversations about science: The socialization of gender inequities? *Developmental Psychology* 39 (2003), 34–47. https://doi.org/10.1037/0012-1649.39.1.34 Place: US Publisher: American Psychological Association.

[85] Milka Trajkova, A'aeshah Alhakamy, Francesco Cafaro, Rashmi Mallappa, and Sreekanth R. Kankara. 2020. Move Your Body: Engaging Museum Visitors with Human-Data Interaction. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376186

[86] Pirko Tõugu. 2021. Motivation for the Family Visit and On-the-Spot Activities Shape Children's Learning Experience in a Science Center. *Frontiers in Psychology* 12 (April 2021), 629657. https://doi.org/10.3389/fpsyg.2021.629657

[87] Arnold P.O.S. Vermeeren, Licia Calvi, Amalia Sabiescu, Raffaella Trocchianesi, Dagny Stuedahl, and Elisa Giaccardi. 2016. Involving the Crowd in Future Museum Experience Design. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. Association for Computing Machinery, New York, NY, USA, 3347–3354. https://doi.org/10.1145/2851581.2856482

[88] Yvonne Vezzoli, Sara Kalantari, Natalia Kucirkova, and Asimina Vasalou. 2020. Exploring the Design Space for Parent-Child Reading. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376696

[89] Lacey N. Wallace. 2022. Associations between Parental Monitoring and Parents' Social Media Use and Social Media Perceptions. *Social Sciences & Humanities Open* 6, 1 (2022), 100294. https://doi.org/10.1016/j.ssaho.2022.100294

[90] H. M. Wellman, D. Cross, and J. Watson. 2001. Meta-analysis of theory-of-mind development: the truth about false belief. *Child Development* 72, 3 (2001), 655–684. https://doi.org/10.1111/1467-8624.00304

[91] Aiyana K. Willard, Justin T.A. Busch, Katherine A. Cullum, Susan M. Letourneau, David M. Sobel, Maureen Callanan, and Cristine H. Legare. 2019. Explain This, Explore That: A Study of Parent–Child Interaction in a Children's Museum. *Child Development* 90, 5 (2019), e598–e617. https://doi.org/10.1111/cdev.13232 _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/cdev.13232.

[92] 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 2023)*. USENIX Association, Anaheim, CA, 399–416. https://www.usenix.org/conference/soups2023/presentation/williams

[93] Pamela J. Wisniewski, Bart P. Knijnenburg, and Heather Richter Lipford. 2017. Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human-Computer Studies* 98 (Feb. 2017), 95–108. https://doi.org/10.1016/j.ijhcs.2016.09.006

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

[95] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300428

[96] 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

[97] Xiaowen Yuan, Hongni Ye, Ziheng Tang, Xiangrong Zhu, Yaxing Yao, and Xin Tong. 2024. RedCapes: the Design and Evaluation of a Game Towards Improving Autistic Children's Privacy Awareness. In *Proceedings of the Eleventh International Symposium of Chinese CHI* (, Denpasar, Bali, Indonesia,) *(CHCHI '23)*. Association for Computing Machinery, New York, NY, USA, 110–126. https://doi.org/10.1145/3629606.3629618

[98] Rita Yusri, Adel Abusitta, and Esma Aïmeur. 2020. A Stable Personalised Partner Selection for Collaborative Privacy Education. In *Adjunct Publication of the 28th ACM Conference on User Modeling, Adaptation and Personalization (UMAP '20 Adjunct)*. Association for Computing Machinery, New York, NY, USA, 47–52. https://doi.org/10.1145/3386392.3397597

[99] Rita Yusri, Adel Abusitta, and Esma Aïmeur. 2021. Teens-Online: a Game Theory-Based Collaborative Platform for Privacy Education. *International Journal of Artificial Intelligence in Education* 31, 4 (Dec. 2021), 726–768. https://doi.org/10.1007/s40593-020-00224-0

[100] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security & privacy concerns with smart homes. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security (SOUPS '17)*. USENIX Association, USA, 65–80.

[101] Shikun Zhang, Yuanyuan Feng, Yaxing Yao, Lorrie Faith Cranor, and Norman Sadeh. 2022. How Usable Are iOS App Privacy Labels? *PoPETs* 2022, 4 (Oct. 2022), 204–228. https://doi.org/10.56553/popets-2022-0106

[102] Xinzhe Zhang, Huaqun Liu, and Shijie Wang. 2021. Design and Realization of Multiple_Platform Digital Museum Interaction System Based on VR&AR. In *2020 4th International Conference on Artificial Intelligence and Virtual Reality (AIVR2020)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3439133.3439136

[103] Leah Zhang-Kennedy and Sonia Chiasson. 2016. Teaching with an Interactive E-book to Improve Children's Online Privacy Knowledge. In *Proceedings of the The 15th International Conference on Interaction Design and Children (IDC '16)*. Association for Computing Machinery, New York, NY, USA, 506–511. https://doi.org/10.1145/2930674.2935984

[104] 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

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

[106] 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 (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300336

[107] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (Nov. 2018), 200:1–200:20. https://doi.org/10.1145/3274469

[108] Heather Toomey Zimmerman, Suzanne Reeve, and Philip Bell. 2010. Family sense-making practices in science center conversations. *Science Education* 94, 3 (2010), 478–505. https://doi.org/10.1002/sce.20374

A APPENDIX

A.1 Interview Protocols

A.1.1 Interview Protocols with Parents. 1 Warm up

- How would you define privacy within the context of your family and daily life?
- Do you ever think of privacy offline?
- Do you ever think of privacy online?
- Do you think there are any privacy challenges in your life?
- Can you share a little about your family's daily routines and activities?

2 Experiences and concerns about family-based privacy problems

- Have you faced any privacy-related situations or dilemmas within your family?
- How do you and your family feel about privacy within your household?
- Are there any specific concerns or challenges you face, especially for children?
- Have there been any conflicts among your family members regarding privacy?

3 Existing educational methods/practice related to these family-based privacy problems

- What measures do you or your family usually take to address privacy issues? Can you share an impressive experience with us?
- Do you believe these measures are sufficient to handle privacy issues?
- Do your family members discuss private matters with each other?
- Are there any specific topics or aspects of privacy that you focus on when discussing it with your children?
- Do you or your family help other families manage privacy issues in their daily lives?

4 Needs of family members in privacy learning and managing in informal learning spaces

- How do you handle situations where your child's privacy is violated or compromised?
- Have you encountered any challenges or difficulties in educating your children about privacy or talking about privacy with your children?
- What are your hopes or expectations about privacy within your family?
- How do you and your family usually learn about technology-related topics, such as artificial intelligence, privacy, and information technology?

5 Experience in informal learning spaces

- Have you studied or learned together with your children outside of school?
- Among all the places you have visited, which one is your favorite one?
- What do you usually do with your children there?
- How do you feel about learning privacy-related topics with your children in these places, such as museums, science centers, or libraries and so on?
- How do you think these experiences in those spaces have influenced your family's overall interest in learning and curiosity?
- In your opinion, do these spaces, just like museums, science centers, and libraries, can be a good place for families to learn about privacy?

A.1.2 Interview Protocols with Children. 1 Warm up

- Can you tell us a bit about yourself and your family?
- Do you have any secrets?

2 Experiences and concerns about family-based privacy problems

- What are your secrets about? You don't have to tell me the exact information because it's your secret, but can you give me an idea of what it might be?
- Have you ever felt like someone is watching your secret too much or that things you don't want others to know are too easy for them to find out?

3 Existing educational methods/practice related to these family-based privacy problems

- How does your family keep your secrets, like your own special box?
- How do you protect your secret?
- Have you ever told someone in your family when you felt like your secret was not safe?

4 Needs of family members in privacy learning and managing

- Do you think you need more help to keep your secret safe and make sure others don't know too much about it?
- What kinds of technology do you use in your everyday life?
- How did you learn to use these things like smartphones or tablets?
- Do you ever talk with your friends or family members about the things you learn or do with technology?

5 Experience in informal learning spaces

- Have you ever visited these places like museums or science centers to learn about new things?
- Can you tell me about the most fun thing you've done at a museum or science center?
- What was your favorite exhibit or activity at the museum or science center?
- Did you talk about what you learned at the museum or science center with your family or friends?
- If you were a designer, how would you design these places for children?