From Knowledge to Practice: Co-Designing Privacy Controls with Children

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

Yaxing Yao
Department of Computer Science
Virginia Tech
Blacksburg, Virginia, USA
yaxing@vt.edu

Abstract

Children born in the digital era are facing increasing privacy risks and the need to control privacy in various contexts, suggesting an urgent need to enhance their privacy literacy. While previous research focuses on developing children's privacy literacy by delivering privacy knowledge, it remains unclear how children process the knowledge and apply it in various privacy situations. Furthermore, children's desire for privacy controls remains understudied. To fill the gap, we conducted two five-day co-design workshops with 11 children (ages 6-11). We uncovered children's sophisticated expectations of everyday privacy management, such as staying aware of their privacy situations, strong authentication methods, and minimal privacy exposure. We further discovered that children translated their privacy knowledge to privacy practices through an iterative *reflection and action* process. We discussed key considerations to support children's privacy literacy development by leveraging this process and offered implications for children-friendly privacy design.

CCS Concepts

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

Keywords

Privacy, Co-design, Children, Privacy Controls

ACM Reference Format:
Lanjing Liu and Yaxing Yao. 2025. From Knowledge to Practice: Co-Designing Privacy Controls with Children. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 22 pages. https://doi.org/10.1145/3706598.3713257

1 Introduction

Children today are born into a world where data collection is ubiquitous due to their access to technology from early childhood [25, 53, 54, 58]. From the moment they interact with digital devices, their data is collected, analyzed, and often exploited [44]. This relentless data collection poses significant privacy risks to children [39, 71, 74]. However, despite growing up in this digital landscape, children are generally ill-equipped to understand and manage such risks due to a lack of sufficient privacy literacy to navigate various privacy situations [42, 46, 65, 71, 95]. Privacy literacy, defined as the understanding of privacy knowledge, critical thinking, and abilities to make informed privacy decisions, is notably deficient among children, especially the younger ones [33, 81].

One alarming consequence of this deficiency is that children may begin to see surveillance as a normal part of life and their personal data as mere commodities [44, 52]. This normalization can have far-reaching implications on their perception of privacy and autonomy [35, 68]. For instance, children might share personal information online without understanding the potential long-term consequences, such as identity theft or cyberbullying [44]. Meanwhile, children do face several privacy risks. Recent reports have highlighted incidents where children's data was compromised, leading to severe repercussions. For example, the hacking of smart home devices has resulted in unauthorized surveillance and even direct communication with children, posing immediate safety threats [49, 76]. These consequences demonstrate **urgent needs to enhance children's privacy literacy** [33, 68] so that they can understand privacy concepts and make informed privacy decisions.

Existing approaches to enhance children's privacy literacy primarily focus on teaching concepts and knowledge [21, 93] via applications [21, 96], e-books [91], and games [32, 55]. While these efforts help children build a knowledge foundation of privacy, they overlook the practical aspects of children's privacy literacy, such as taking actions to protect themselves from various privacy risks in real life. It is not clear how children translate their privacy knowledge into everyday privacy practices and what kinds of privacy controls they desire when they are able to implement them. This is an important step towards enhancing children's comprehensive privacy literacy and preparing them to handle complex privacy situations. This paper aims to fill the gap and ask the following research questions:

RQ1: How do children translate their privacy knowledge into everyday privacy practices?

RQ2: What are children's needs and expectations for privacy controls?

To answer the research questions, we conducted two five-day co-design workshops with 11 children (ages 6-11) in total as well as their parents. Co-design has been widely used in Human-Computer Interaction (HCI) and privacy communities to study users' needs [12, 84, 85]. In the Children-Computer Interaction (CCI) community, co-design is also a common method to capture children's perspectives, especially about privacy [32]. This method allows us to prioritize children's needs and understandings by empowering them to take ownership of the process and outcomes and foster their autonomy in privacy [55]. Additionally, recognizing the importance of

CHI '25, Yokohama, Japan

ACM ISBN 979-8-4007-1394-1/25/04
https://doi.org/10.1145/3706598.3713257

parental involvement in privacy education and practices [2, 35, 66], we also invited parents to participate as co-design partners on the last day of the workshops.

We used a series of co-design activities, including the *big paper* techniques [4, 79] and *focus groups* as data collection techniques to explore children's perceptions of privacy and their needs and expectations of privacy controls. Our findings, rooted in the rich data we collected, revealed children's varying levels of perception across different privacy contexts—interpersonal, institutional, and commercial privacy. Additionally, we uncovered children's expectations of everyday privacy controls, such as staying aware of their data processing and broader contexts of their interaction, strong authentication methods, minimal privacy exposure, and real-time and contextual assistance when they make privacy decisions. We also noticed a discrepancy between children's sophisticated privacy control expectations and their simple privacy control strategies when facing privacy risks, such as unplugging devices. Then, we highlighted three fundamental aspects of children's needs for privacy controls: a sense of security to feel safe and protected, the ability to detect privacy threats accompanied by clear and understandable feedback, and simple, actionable solutions to effectively address risks. Finally, we characterized an iterative reflection and action process through which children internalized privacy knowledge and translated it into practical control measures.

This paper makes three key contributions. First, through two co-design workshops with 11 children, we uncovered children's expectations of desired privacy controls. Second, while previous research focuses on educating privacy knowledge and concepts to children [32], our work extends this landscape by specifically examining how children translate privacy knowledge into practices. We further discussed the opportunities to support this process to enhance children's privacy literacy development. Finally, we drew implications on children-friendly privacy designs.

2 Related Work

2.1 Privacy Education for Children

Prior work has shown that children face significant privacy risks online, including identity theft and cyberbullying [44, 52]. A promising approach to help children address these risks is through privacy education. Research has primarily focused on three types of interventions: (1) applications [21, 89, 96], (2) games [55], and (3) interactive e-books [91]. Generally, the applications offer some privacy guidelines and knowledge for children to enhance their cognitive, situated, and thinking of online privacy issues, especially privacy online risks [89].

Educational games and e-books offer an interactive privacy learning experience for children. For example, *The Watches* is a computer game/board game hybrid, set in a fictional 'Union City', where children act as secret agents to explore privacy-related scenarios [55]. "Cyberheroes" is an interactive e-book that teaches children about various online privacy issues [91], while DOPA books combine physical and digital elements to help early adolescents learn about informational privacy [86]. These interactive methods engage children actively in the learning process, making privacy concepts relatable and easy to grasp.

However, privacy literacy involves not only privacy knowledge but also making informed privacy decisions. Rather than simply listing do's and don'ts, effective privacy education should teach children to make autonomous decisions as they mature [32]. In games, children often follow instructions from educators, parents, or game guidelines, limiting their ability to learn about privacy independently. Ignoring children's autonomy in the learning process can reduce the effectiveness of these tools. E-books face similar challenges, often becoming outdated due to the rapid evolution of privacy issues online [86]. Moreover, they tend to present a fixed view of privacy rather than encouraging children to reflect on and shape their own privacy attitudes [19]. Privacy is not just a concept to be learned; it is an active, everyday practice [33]. The ultimate goal of privacy education is to empower children to control their privacy in complex, real-world contexts. Understanding how children translate privacy knowledge into practical control is essential for helping them with privacy practices.

2.2 Privacy Design for Children

Children's privacy is under significant threat in the digital age, as apps and platforms often fail to provide adequate support. For example, many children's apps routinely share personal data with trackers and ad networks, despite regulations like COPPA (Children's Online Privacy Protection Rule), which prohibit such practices [3, 57]. Research reveals that most family-oriented apps use trackers, with many violating data privacy rules, creating long-term risks for children [57]. While developers often aim to protect young users, compromises are frequently made due to limited monetization options and the lack of clear privacy guidelines [22]. Additionally, emerging technologies such as wearables present new and evolving privacy risks for children [9, 37]. Despite these growing challenges, current privacy designs fail to address children's unique needs effectively. Privacy features and request notifications are primarily designed for adults, making them inaccessible or ineffective for children [70, 73]. This gap highlights the lack of child-friendly privacy design in today's digital environments, where children's concerns are often overlooked, reinforcing the notion that they are "not seen, not heard in the digital world [73]."

Moreover, there is a shortage of clear design guidelines tailored specifically to children's privacy needs. Dempsey et al.'s research on children designing privacy warnings demonstrates the value of child-centered methods in improving privacy design. By involving children in creating privacy-related warnings, organizations could develop more meaningful and effective tools to communicate online risks to young users [19]. However, efforts to address these issues are hampered by insufficient regulatory and design support for children's privacy rights. There are growing calls for stronger regulatory interventions to ensure more robust protections that consider children's unique vulnerabilities in the digital landscape. Addressing these challenges requires not only improved design practices but also prioritizing children's privacy needs.

2.3 Co-designing with Children

Since Druin introduced a widely adopted model for involving children in the design process—where children can take on roles as users, testers, informants, or full design partners [20] — co-design

has become a prevalent method in HCI and CCI research for understanding children's needs and creating innovations for them. While the roles of users and testers focus primarily on gathering feedback or input at the end of the design cycle, the roles of informants and design partners emphasize deeper involvement, positioning children as equal stakeholders alongside adult designers [20]. Co-design empowers children to propose solutions [61], facilitates a deeper understanding of their needs [80], and encourages reflection on technology use [13]. For instance, Wilson et al. used co-design to help verbal children express themselves through actions and interactions [80], while Wang et al. explored children's expectations for managing datafication through 10 co-design sessions [79]. Additionally, Woodward et al. examined children's conceptual models of intelligent user interfaces [83].

In designing for children's privacy, the principle "*Nothing about us without us*" emphasizes the importance of prioritizing children's perspectives on privacy and security issues, rather than dismissing their views as immature or naive [34]. One example is "*The Watchers*," a hybrid computer and board game where children, acting as secret agents, explore privacy-related scenarios [55]. Similarly, Kumar et al. examine how games and storytelling can shape resources for teaching children about online privacy [32]. In our study, co-design with children enabled them to act as co-creators, allowing us to learn their perspectives on various privacy contexts and their needs and expectations of privacy control. On the other hand, co-design activities also contributed to children's literacy development like empathy [77] and nature literacy [78]. By involving children in several co-designing activities related to privacy, we provided a relaxed environment where children could develop their privacy literacy and allowed us to observe how they internalize and apply privacy knowledge in practice.

3 Method

To answer our research questions, we conducted two five-day design workshops with 11 children (6-11 years old) to explore their understanding of privacy, as well as their experiences and expectations of managing their privacy and privacy learning support. Recognizing the importance of parental involvement in children's privacy education [2, 35, 66], we invited the parents to join as co-design partners in the final design session. Our study has been carefully reviewed and approved by our university IRB office.

3.1 Participants Recruitment

In this study, we aimed to recruit children between 6 and 11 years old. We focused on this age range as literature has suggested this range to be a critically important time to educate young children about privacy. This is because children start to gain some knowledge and care about the basic idea of online privacy as young as 6 years old [47]. Up to 11 years old, children value their privacy but cannot fully understand what it means to be private online, and also have flawed reasoning behind their understandings [6, 50, 91]. They also show less competence in managing their online privacy settings than older teens (aged 12-17) [8]. Prior work has primarily focused on supporting privacy and security for children over age 12 [1, 51]. Because of these reasons, our study focused on children between 6 and 11 years old to fill the critical gap in the literature.

Considering the interactive nature of the co-design workshops, for the best results we aimed to only recruit in-person participants. We posted our recruitment flyers in our local communities (e.g., bulletin boards in public libraries, community centers, and playgrounds) and our local social media groups. We recruited 11 children in total; all children speak English and come from the United States of America. We then divided the children into two co-design groups based on their ages, family backgrounds, and other demographic information to ensure diversity in each group. Table 1 summarizes the details of participants' backgrounds and their group allocation.

3.2 Co-design Workshops

We held two co-design workshops in July and August of 2024. The two workshops followed the same procedure. Each workshop contained five co-design sessions, spanning five consecutive days. Each design session had a self-contained topic and a set of activities. The outcomes from the previous day shaped the activities of the next day. Each design session lasted around 3.5 hours. Next, we introduce the co-design workshop procedure and activities in detail. The complete study guide and detailed activities in each design session can be found in the Appendix 3.

3.2.1 Design Session 1 (DS1, Day 1): Understanding Children's Conceptualization of Privacy. The goal of DS1 was to set up children's role as technology designers (as opposed to technology users) and understand their current awareness of privacy and how they manage it in their daily lives. We began the first day by introducing the children to the design session and asking everyone to briefly introduce themselves to the group. We then moved on with a design activity to initiate the discussion of privacy. To do this, we adopted a *scenario centers* approach by asking the children to design a "lock" to protect their privacy in a range of scenarios that the children were familiar with, such as social media (e.g., Instagram), communication apps (e.g., Google Chat), video platforms (e.g., YouTube, TikTok), learning devices (e.g., Chromebook), and smart home devices (e.g., Amazon Echo, smart cameras). This activity not only provided us with insights into children's perspectives on privacy and protection but also introduced them to the role of a designer and encouraged them to proactively think about how to design for privacy protection.

To engage the children deeply with various privacy concepts and help them understand abstract privacy concepts, we narrowed the wide range of scenarios down to one specific context (in line with prior work [79], i.e., *smart home devices* for the two subsequent design sessions. We chose smart homes primarily for the following two reasons. First, as context is essential for children's comprehension of privacy [32], investigating how children interact with privacy risks in familiar environments is critical for creating effective privacy protection strategies. Through DS1, in line with the findings from prior work [14, 70, 72], we noticed that all children were familiar with smart home devices, with some of them considering smart home devices as an integral part of their family lives. As a result, using smart homes as a scenario provides a unique opportunity to engage all children actively in the design process. Second, smart home devices offer a special context for both online and offline challenges, especially for children [43, 90, 97]. For example, children may use smart speakers to access online information

ID	Age	Grade	Gender	Ethnicity	Speakers Usage	Parent involved	Workshop
Emma	9	3	Female	Asian	Extensive	Mother	WS1
Ethan*	7	2	Male	Asian	Frequent	Mother	WS1
Grace*	7	2	Female	Asian	Frequent	Grandmother	WS1
Leo#	9	4	Male	Asian	Frequent	Mother	WS1
Lucas#	6	1	Male	Asian	Minimal	Mother	WS1
Mia	10	5	Female	Asian	Frequent	Father	WS2
Chloe	9	4	Female	White/Asian	Frequent	Mother	WS2
James	11	5	Male	Asian	Extensive	Mother	WS2
Lily	10	4	Female	Asian	Extensive	Mother	WS2
Jack	9	4	Male	Hispanic/Latino Origin	Frequent	Father	WS2
Henry	8	3	Male	White	Minimal	Mother	WS2

Table 1: Participants demographics. Siblings are denoted by * and #; C04 and C05 shared their mother during DS5. "Speakers usage" means the child's familiarity and use of smart speakers, such as Amazon Echo, Google Home, or similar voice assistant devices; Minimal: they've tried using one a few times, but they don't engage with it regularly. Moderate: they use a smart speaker occasionally, but it's not a significant part of their routine. Frequent: they use a smart speaker regularly for tasks like listening to music or asking questions. Extensive: they rely on a smart speaker daily and understand how to use more advanced features or settings.

(e.g., weather, asking questions) and purchase items. At the same time, smart home devices are equipped with various sensors (e.g., microphones, cameras), enabling them to collect data of family members and raising significant privacy concerns [27]. As a result, smart homes naturally present a complex environment with different aspects of privacy issues, such as online and offline privacy, children's privacy, and the privacy of other family members, and different types of data collection.

In the following DS2 and DS3, we situated our design activities in the context of smart homes to dive deeply into children's understanding of privacy and lay a solid foundation for different aspects of privacy (as discussed in the next two sections). Building on the knowledge, we further encouraged children to broaden their perceptions and designs to broader privacy challenges across various technological contexts in DS4 and DS5.

3.2.2 Design Session 2 (DS2, Day 2): Identifying and Mitigating Privacy Concerns. The activities in DS2 aimed to understand how children control their privacy in their everyday lives. Children first freely interacted with an Amazon Echo while we observed their interaction. They then discussed potential privacy issues they may encounter in their interaction and collaborated with us to design possible ways to mitigate these issues. We used a series of design techniques to facilitate the collaboration. For example, we used *Big paper* technique, a form of scenario-based design in which each design group uses props (e.g., removable whiteboard, easel pads, and craft materials) to act out a scenario [4, 79]. To understand children's desired privacy control mechanisms, we further asked the children to design a button, a tangible artifact that would help them protect their privacy while using Amazon Echo.

3.2.3 Design Session 3 (DS3, Day 3): Understanding Privacy Dynamics Beyond Individuals. In DS3, our goal was to continue exploring children's understanding of privacy in smart homes and expanding the concept of privacy beyond that of individual users, then conduct co-design activities to understand how children would design privacy protection mechanisms with a broader conceptualization

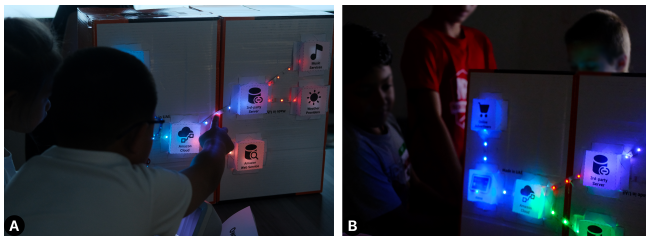

Figure 1: Children interacted with the prototype during DS 3. A. The first workshop. B. The second workshop.

of privacy. To help children understand the smart home ecosystems beyond individual users, we designed an interactive prototype that demonstrated how smart speakers collect, transmit, and process their conversation [67] with other stakeholders in this ecosystem. This technique was inspired by prior work [79, 87]. For example, Wang et al. used mockups of changes to mechanisms in the YouTube to facilitate children's discussion on their needs when navigating through datafication practices and deriving age-appropriate design implications. Given that many privacy concepts are highly abstract and hard to understand for children, we intended to use the prototype to clarify abstract privacy concepts and as a prompt to inspire children's design ideas.

The design of the prototype in DS3 is grounded in Kumar's privacy literacy framework [33]. This framework defines *information flow* as the foundational step in helping children understand privacy. As such, the prototype focuses on visualizing the information flow in a simplified smart home ecosystem (Figure 1).

At the beginning of DS3, we presented the prototype to the children and allowed them to freely interact with it. After every child had a chance to try the prototype, we conducted a *focus group* in which the children reviewed the prototype and brainstormed their own ideas to revise the prototype. The results shed light on children's desired privacy knowledge, particularly related to the privacy of stakeholders beyond themselves.

3.2.4 Design Session 4 (DS4, Day 4): Empowering Privacy Control. The first three design sessions focused on building children's foundational privacy knowledge. The goal of DS4 was to understand children's desired privacy controls. We started the day with a *focus group, in which we guided the children* to recap the foundational privacy knowledge from the first three days. We then encouraged them to design a tool that "teaches other children the most important thing when controlling your privacy", allowing us to closely examine children's needs and priorities in privacy controls. During the process, we asked the following guiding questions to initiate the design: *1) "Who will use your design? Why?" 2) "What do you think is the most important thing about privacy?" 3) "How will your design teach them? Show or provide something?" 4) "When and where will they use your design?"* We assisted them in articulating their ideas and provided other help (e.g., cutting cupboards) as needed.

Upon completion, we asked everyone to create a poster to organize their thought process and present their designs as a way for the children to document and reflect on the process. In the meantime, the poster was also used in the forthcoming activities in DS5 to receive feedback from their parents.

3.2.5 Design Session 5 (DS5, Day 5): Refining and Presenting Privacy Solutions with Parents. The goal of DS5 was to allow the children to reflect on their experiences in the first four days and iterate on their designs of privacy controls with their parents. We started by recapping the content of the previous four design sessions with both the children and their parents. Then, the children presented their poster to their parents and other children and answered any questions they may have. Following the presentation, the children and their parents worked together to refine their design ideas, prototypes, and posters, before giving a final presentation and participating in a Q&A session. This activity gave the children an opportunity to iterate their privacy control design with their parents and, at the same time, provide us with insights into how parents' involvement impacts children's privacy learning and control.

Upon completion, we offered each participating child $100 and each participating parent $25 Amazon gift card. Additionally, we also offered all participants the opportunity to participate in a series of follow-up educational and research programs hosted by our research lab, as all participating children and parents considered the design workshop "educational" and "insightful."

3.3 Data Analysis

We recorded the video and audio for the entire workshop with the children's consent and their parents' permission. We also photographed all children's sketches and prototypes and took notes as needed. In total, our study resulted in 35 hours of video recording and 892 images. We first transcribed the videos using Kaltura[1], and then the co-authors reviewed and corrected the transcriptions. We followed previous research practices to analyze the session recordings [69, 87]. We captured both textual content and relevant visual data (e.g., a child pressing a button on the Amazon Echo or using a camera cover) and linked these details to the children's sketches and field notes. The remaining co-authors then verified the accuracy of the transcriptions and the established links. We then organized all the data chronologically based on the design sessions (i.e., all data belonging to one design session was grouped) and the participants (i.e., all data belonging to one participant across five days was grouped, such as each participant's design ideas, sketches, prototypes, and field notes). This approach provided a comprehensive view of the workshop and enabled us to trace each participant's development in privacy literacy over the sessions.

We then conducted a thematic analysis on the transcriptions and notes [7]. For the visual data, we applied narrative analysis to construct participants' design narratives and explored how they visually represented their design ideas and learning processes [59]. Two coders thoroughly reviewed all video transcripts and images multiple times and coded the data. The research group analyzed the data from the first workshop collaboratively and created an initial codebook with preliminary codes for each design session (e.g., privacy control expectations, judgments on privacy contexts, and privacy protection practices). In this collaborative process, the group discussed any disagreement thoroughly to reach a complete agreement. This process also aimed to ensure that we covered all the aspects of our data and the links among them, given the multiple types and sheer volume of our data. Then, one researcher coded the second workshop independently using the initial codebook. Upon completion, the group reviewed the codes together, discussed any disagreements, and refined the codebook as needed until a full agreement was reached. In this process, we did not observe new clusters of codes emerge, suggesting that thematic saturation had been reached and that our data effectively covered the key aspects of our research questions [62]. As we collaboratively completed the coding in multiple rounds and reached a complete agreement, the inter-coder agreement was not required [45]. The codebook can be found in the Appendix 2.

3.4 Ethical Considerations

As our research involved minors between the ages of six and eleven, we paid extra attention to our research ethics. Before the workshop, 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. During the workshops, similar to prior work [35, 36], we developed three strategies to help children protect their privacy: (1) we employed child-friendly language to remind them not to share sensitive information; (2) when discussing sensitive topics like passwords or personal privacy, we instructed the children not to share specific details with us first, then we had a discussion; (3) if a child showed any tendency or behavior toward leaking private information, we immediately reminded them not to share private information. We then reported the incident to the parents after the session. Following the workshop, we conducted follow-up interviews with all parents to answer any questions they had and provided suggestions as needed.

When storing the data for analysis, we followed the guidelines from our university technology Office closely by using university-approved software and cloud services, using pseudonyms or participant codes instead of real names, and anonymizing personally identifiable information during analysis and reporting.

[1]Kaltura is a FERPA-compliant video content management system approved by our university technology office and IRB office. The use of Kaltura was included in the consent form and assent form for participants' awareness.

3.5 Limitation

There are various limitations in our study. First, we had 11 child participants, which might seem to be a small number; however, this is consistent with prior participatory design research with children (e.g., [5, 32, 69, 88]). We held continuous five-day workshops. Compared to single or widely spaced sessions, continuous workshops supported sustained and coherent learning for the children, allowing them to reflect on their experiences. This format also enabled us to observe the children's complete learning process. Since this study required in-person participation, we recruited children from the town in which our university is located. As a result, our participants and their families are skewed toward highly educated, Asian-affiliated families. This demographic focus, common in similar studies [69, 87], limits the generalizability of our findings. However, our participants represented different levels of prior knowledge about privacy, allowing us to collect diverse insights. Future research can address this limitation by recruiting a broader demographic to explore potential cultural differences in privacy perspectives. Additionally, as a qualitative study, our research shared the limitations common to qualitative methods. It lacked generalizability, and personal experiences and interpretations can introduce bias and constraints. Although we encouraged children to share openly, their responses may still have been influenced by peer pressure, social expectations, or other personal factors [18].

4 Results

In this section, we present findings on children's varying levels of perception across different privacy contexts, how they translate privacy knowledge into practices, and their expectations of privacy management and protection.

4.1 Understandings of privacy

The first theme is related to children's varying levels of privacy perception across different contexts. We further categorized these perceptions into three main categories based on Livingstone's privacy framework, including interpersonal privacy, institutional privacy, and commercial privacy [66]. We found that children played dual roles depending on the context, indicating their multifaceted view of privacy as something that shifts across interpersonal, institutional, and commercial settings. In the following sections, we present the details.

4.1.1 Interpersonal Privacy: Understanding and Curiosity. *Interpersonal privacy* refers to privacy between an individual and other individuals or groups. The children in our study demonstrated a strong understanding of interpersonal privacy in three contexts, i.e., in their rooms, regarding their passwords and accounts [2].

Interpersonal Privacy Ties to Children's Physical Privacy. Children's understanding of interpersonal privacy is often strongly associated with physical privacy. In DS1 of both workshops, when we asked children about their thoughts on privacy, all their answers associated the term "privacy" with examples like body privacy, bathroom, and their rooms, echoing the finding of Oates et al [48].

Testing Interpersonal Privacy Boundaries with Passwords. Interestingly, despite their awareness of privacy, many children attempted to test the boundaries of privacy by trying to break other family members' passwords. Children often viewed this as a challenge, especially when their families set strong privacy boundaries (e.g., consistently refusing to grant children access to their accounts). Sometimes, family members do not have strong protection for their personal information, especially passwords. Children, driven by curiosity, found loopholes and exploited them both offline and online. For example, when we talked about passwords, Leo complained about how his family tried to keep passwords away from him, which only motivated him to figure them out: "*Every time my family tries not to let me know what their passwords are...Sometimes, I figure them out from older passwords, and they forget they're trying to keep the passwords away from me and accidentally say that while I ask them for the passwords. On my dad's computer, he said ****[3]. *But then I figured it out because he forgot about it again... I figured out the new password is ****" (Leo, 9, M, DS1, WS1).

4.1.2 Institutional Privacy: Blind Trust. *Institutional privacy* refers to privacy between an individual with a public or third sector (not-for-profit) organization. In our study, the children discussed their privacy perceptions about their schools and the online learning devices (e.g., Chromebooks) provided by their schools. They showed very little concern about their information (e.g., names, ages) being collected by the devices provided by schools and online learning platforms on the devices. For instance, Lily said, "*They (Chromebooks) know my name, my age, my last name, and probably they know more. I'm OK with it*" (Lily, 10, F, DS1, WS2).

We consider this phenomenon as children's "blind trust" towards certain institutions, particularly schools. After learning privacy concepts in class, they tend to develop trust in the institution without critically questioning the extent or limits of that trust. Interestingly, we noticed that this blind trust extended to us (the researchers), as the children considered the researchers as university representatives, and thus were trustworthy. For example, when we asked the children if they had their own passwords, Lucas told us the password of his iPad[4]. When we asked why, Lucas just said, "*because you are the teacher, from the university*" (Lucas, 6, M, DS2, WS1).

4.1.3 Commercial Privacy: Ambiguity and Uncertainty. *Commercial privacy* refers to privacy which is between an individual and a commercial (for-profit) organization ("commercial privacy"). Compared to institutional privacy, the children were more sensitive to their information being collected by commercial entities (e.g., Google, Amazon, and social media companies). In DS3, a few children discussed the commercial privacy issues related to selling personal information. James said, "*They're not really hackers. They're just advertising,*" (James, 11, M, DS3, WS2) while Chloe added, "*So then they can sell the information to Spam also. And then Spam will call you*" (Chloe, 9, F, DS3, WS2).

Yet, it should noted that children often do not know the details regarding commercial privacy. For example, many children were uncertain about "who" were the entities that collected their data, thus

[2]For children, passwords encompass both accounts and devices, but when they refer to "accounts," they are specifically talking about online accounts, aligning with Zhang-Kennedy et al [94].

[3]When the child mentioned such passwords, we stopped them, advised them not to share passwords again, and deleted the password from the recording.

[4]Similar to prior incidents, we paused the session, explained to the children, and removed the information from the recordings.

often mixed different companies. During a discussion about a boy using Amazon Echo, when asked who would collect the boy's data, many children were unsure, with Jack responding, "*Google!*" (Jack, 9, M, DS1, WS2).

4.2 Children's Expectations in General Privacy Management

One key finding of our study relates to children's expectations on how to manage their privacy and protect themselves from various privacy risks. Their designs centered around their right to know about privacy-related matters, preferences for strong authentication, and their desired support for privacy decision-making.

4.2.1 Expectation: Stay Aware. Through their designs, the children showed a strong desire to know different aspects of their privacy. We identified two key aspects of their desires, including understanding what has happened to their data and receiving potential risk notifications, and grasping the broader context behind interactions, such as the information flow and the stakeholders involved.

Staying Informed of Potential Risks. Children expressed their desire to receive timely notification about potential privacy risks. They wanted to know any signs related to possible privacy risks or leakages, particularly those that might compromise their personal information or physical safety. For instance, in DS3, as Figure 2A shows, Leo described a lock that , "*if you set the camera to destroy mode, it will see if the person is an intruder or not*" (Leo, 9, M, DS3, WS1). Mia designed a lock that alerts users when incorrect passwords are entered (Figure 2B). Grace suggested a recording system for locks, where users can retrieve and review messages the next day to learn what happened. Children also emphasized the importance of receiving timely notifications about privacy risks. Mia proposed a system that uses a tracker and camera to send alerts if someone steals a key. Ethan, Grace, and Mia designed a system that sends a notification if a key isn't used within a set time frame, "*There's going to be a lock and a time limit screen. And then, right here, there is going to be a key to open it. And then, if the person doesn't open it, it's going to send a notification*" (Mia, 10, F, DS2, WS2). Lucas and his mom created a button with a "beep" sound to alert him to potential online privacy risks.

Understanding a Big Picture of the Privacy Ecosystem. Even though most children showed a basic level of understanding of privacy, they still expressed curiosity about the "big picture" of the ecosystem regarding their privacy, such as which entities were involved in the ecosystem and how data flew among these entities. We learned this need from several children's designs. For example, Leo wanted more details about the various stakeholders involved in information transfers , "*I wanted more examples, like fake products, fake information, and fake warnings*" (Leo, 9, M, DS3, WS1). Emma proposed a website that explains the data transfer process behind Amazon Echo. Ethan suggested a 3D model to visualize the flow of information, while Henry used a car analogy to illustrate the direction of data flow, "*I think we should put a car on here [pointed his finger at the information flow]. There's a switch. If you look in here, it goes on here [pointed his finger at an information recipient]*" (Henry, 8, M, DS3, WS2). As Figure 3B-i shows, James created a visualization to show where personal data goes when posted on social media.

4.2.2 Expectation: Strong Authentications. All children in the workshop have developed a sense of strong authentication to safeguard their personal information. In their designs of locks and private use of Amazon Echo, they expected to have similar measures to safeguard their private information. They primarily suggested three types of authentication, i.e., biometric authentication, multi-step authentication, and adaptive authentication.

Biometric Authentication. The majority of children showed a strong preference for biometric authentication methods, such as fingerprints, facial recognition, and iris scanners. Emma, Jack, Chloe, and Leo also chose biometric authentications when designing their locks (Figure 2). They believed that passwords and keys could easily be lost, forgotten, or cracked, whereas biometrics, being unique to each individual, provided a more secure and trustworthy protection method. For example, Emma designed a lock for money by using a tail printer (Figure 2C-i), and she explained, "*But they might steal the key. Yeah, but they can't do the tail print*" (Emma, 9, F, DS1, WS1). Leo envisioned a system that could recognize faces and even adapt to changes, such as recognizing a newborn as they grow. "*You have to take photos and then install them. It's not that hard. So they [the lock and the system] know who it is, and you could always make new people if you have a newborn*" (Leo, 9, M, DS1, WS1). He also selected AI to program this system because he wanted it to update continuously, ensuring security while adapting to changes in appearance.

Multi-Step Authentication. Children's designs suggested their expectations of using authentication that combines multiple methods for added security. Jack designed a lock that required four steps: a rotating mechanism (Figure 2D-i), a password (Figure 2D-ii), an eye scan (Figure 2D-iii), and a fingerprint scan (Figure 2D-iv). Emma created a shell for her toy monkey's use of smart home devices, which involved a keyhole, a trail print, and a password, "*This should be a wire that you plug in, you also plug it into the lock, and then you go to upload tail print, and then you click upload tail print, and you put your tail print on the circle, this scoring shows upload tail print, it's loaded, it's 80%. Once it's 100%, it's loaded, and you can use your tail print to unlock it. You have to go through the three stages*" (Emma, 9, F, DS2, WS1). Grace devised a personal box that used a key, password, and hidden battery placement, only known to her, to secure her privacy, "*I pick up the key, and I get a door password, and I put a battery for the door password*" (Grace, 7, M, DS5, WS1).

4.2.3 Expectation: Minimal Privacy Exposure. When the children were prompted to design a privacy-enhancing feature for smart home devices in DS2, they expressed a clear desire to minimize data exposure and control the information collected by smart devices. Emma, for instance, suggested deleting all data Amazon Echo collects within five hours, explaining that this would prevent someone from hacking into the device and using personal information for malicious purposes. She emphasized, "*So no one can hack into Alexa...there will be privacy*" (Emma, 9, F, DS3, WS1). James echoed similar sentiments, advising users to avoid sharing private information online, not to create accounts, and to avoid engaging in comment sections for safety.

To some extent, children demonstrated high sensitivity to camera usage in smart devices. Henry stated that he only used his smartwatch's camera because it was not connected to the Internet.

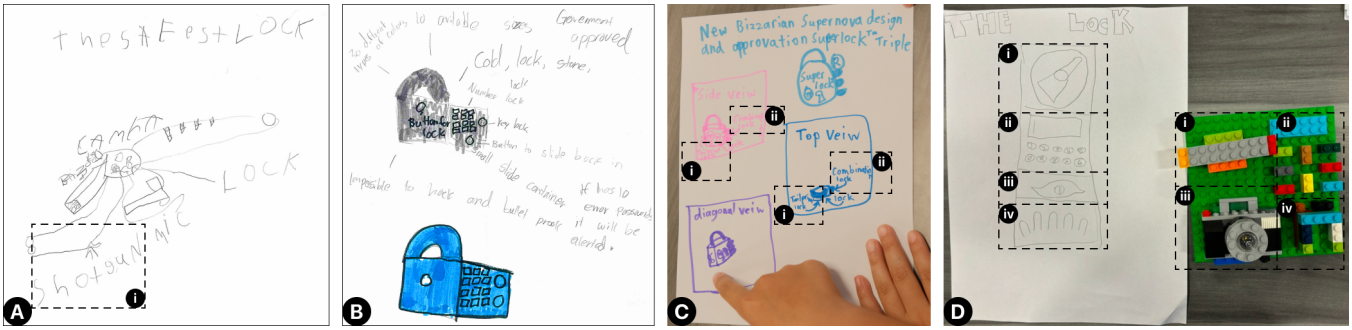

Figure 2: Children's sketches and prototypes of lock designs: A. Leo's: A lock equipped with a camera for facial recognition and a shotgun to deter intruders. B. Mia's: A lock featuring a keyhole and password. It alters functionality if compromised. C. Emma's: A lock designed for monkeys, incorporating a keyhole and a tail pointer. D. Jack's: A multi-component lock with a password, eye scan, fingerprint scan, and rotating mechanism.

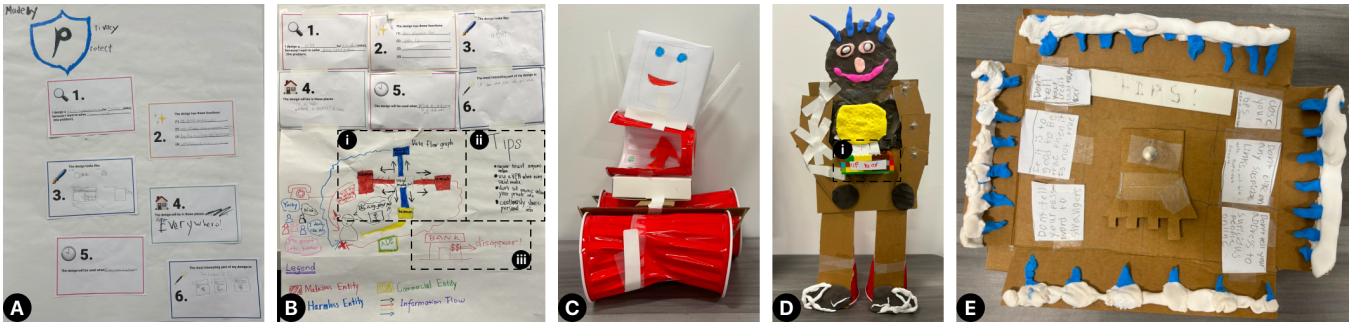

Figure 3: Children's posters and prototypes designed to teach others about privacy: A. Emma's: A button that eliminates spam, phishing attempts, and hackers. B. James's: A visualization showing the flow of information on social media, accompanied by a story created with his mom. C. Henry's: A robot with pointers to identify and present true and false information online and offer real-time assistance when surfacing online. D. Lily's: A robot named Scammer Scanner with a daily privacy tip box that helps detect scammers and alerts users through a speaker. E. Jack's: A privacy tip board that automatically provides suggestions for teachers to educate students about privacy.

Lily said, "*Alexa can hear you, something that was about you. Alexa can see you do anything if you forget the camera. Someone can hear Alexa. So they know about you*" (Lily, 10, F, DS2, WS2). James added, "*Alexa can see your house through the camera if you'll turn it off. So people know where you are, technically. Put that near a window, or they can see the approximate place*" (James, 11, M, DS2, WS2). To address their concerns, children demonstrated creative ways to limit the data collection and capabilities of devices. Chloe designed a box with a one-way mirror for the cameras on smart home devices, so "*It can't see anything, but you can see through*" (Chloe, 9, F, DS2, WS2). Similarly, both Lily and Henry designed a double-layered box to prevent the cameras on smart home devices from seeing or collecting visual information. In another approach, Emma and Leo designed a button for smart home devices, so "*you could just mute it*" (Emma, 9, F, DS2, WS1), giving users control over when smart home devices can listen or watch.

Children's awareness of camera privacy heightened after discussions in DS2. When interacting with Amazon Echo in DS3, Ethan proactively turned off the camera and got agreement from all the children. Lily, who designed a robot to provide computer-use assistance, specifically pointed out that "*there is no camera on the robot, so it can't see you*" (Lily, 10, F, DS5, WS2), further demonstrating the children's preference for devices that limit visual data collection (Figure 3D).

4.2.4 Expect Real-Time and Contextual Assistance to Make Privacy Decisions. In addition to understanding the privacy situations, children also expressed a clear need for real-time, context-based support when making privacy-related decisions. Many children needed assistance, especially when adjusting privacy settings or deciding how to share personal information. Ethan envisioned a website that provides privacy knowledge and specific recommendations for privacy management. James designed a system for social media that helps users understand where their data goes after posting or commenting (Figure 3B-i). Additionally, as Figure 3B-ii shows, he offered practical privacy tips, such as never trusting strangers online, using VPNs when browsing social media, and avoiding the sharing of personal information. Figure 3E shows that Jack designed a privacy tip board that automatically provides suggestions when students need to make privacy decisions.

In DS5, by involving parents, we also gained insight into what parents expected for their children's privacy management in their daily lives. Parents echoed these sentiments, expressing more support for their children, particularly when navigating online spaces. As Figure 3D shows, Lily proposed a robot equipped with a speaker to notify users of potential scams, describing it as, "*It can help you know if there's a scammer, it has a speaker to let you know about the scammer*" (Lily, 10, F, DS5, WS2). Lily's mother extended this idea with a "Tips Box" (Figure 3D-i), offering children privacy-controlling tips every day.

Henry designed a robot that assists with online shopping, telling users whether to input certain information, such as their address (Figure 3C). His mother added that the robot could also guide users on which data was necessary to share for purchasing (e.g., address for delivery) versus information that could be withheld (e.g., phone number or birth date). This design helps users make informed decisions about what to disclose, ensuring they balance privacy with practical needs like receiving packages.

4.3 Children's Expected Privacy Protection Process When Facing Risks

In addition to children's general expectations of privacy management strategies, we also noticed children's expectations of how they should handle privacy issues when facing privacy risks.

4.3.1 Sense of Security. Children expressed a strong desire to feel secure when confronting privacy threats. Many envisioned "omnipotent designs" to safeguard their privacy. For instance, Grace designed a lock with a "*super spy guy*" who would physically remove a stranger if they tried to breach the lock, while Leo envisioned a button that would create a 100-meter radius jam to disable any incoming privacy threats like viruses or hackers. Mia also imagined a button that could be activated when privacy threats like hacking or scamming were detected. She described it as "*will be used when you are hacked or scammed, bugs and more are found or detected. The button can change and reset passwords, hackers, et cerate*" (Mia, 10, F, DS5, WS2). These designs highlight the importance of making children feel that their privacy is being actively protected.

4.3.2 Privacy Threat Detection and Understandable Feedback. Many designs focused on autonomous detection paired with actionable alerts, highlighting the importance of tools that could intelligently identify and address privacy threats. These privacy threats include fake information, scammers, hackers, and spam. Henry envisioned a robot that could discern truthfulness online, stating, "*I made a robot that will tell you if what it is true or if it [is not]... people don't tell you what's true on the computer*" (Henry, 8, M, DS5, WS2). Leo iteratively refined his design across sessions. In DS4, he suggested a warning system: "*A warning that will say you are getting hacked. So then you can just press*" (Leo, 9, M, DS4, WS1). By DS5, Leo added further sophistication, explaining, "*If a device is trying to connect to your device, but that device is connected to a different Internet away from yours, or close to yours, it will warn you that somebody is trying to hack into your device*" (Leo, 9, M, DS5, WS1). Lily designed a robot that detects scammers and alerts users through a speaker. Her mother expanded on this by AI-supported functionality (Figure 3D), noting, "*And because it is AI-supported like my daughter said, now it can talk with you. It can help you and it can explain to you why this is spam and why this is not spam*". These concepts illustrate children's and parents' desire for proactive systems that detect privacy threats and also provide understandable, real-time feedback.

4.3.3 Easy to Handle. Once aware of potential privacy threats, children preferred simple and intuitive tools to neutralize them. For example, in Leo's design, after knowing the hacker, you just need to press the button then the hacker would be removed. Emma developed a "*Bug Clear Button*" (BCB) that users could press to eliminate spam, phishing attempts, and hackers. She explained her idea as "*If you have bugs you just push the BCB and all the bugs are gone*" (Emma, 9, F, DS5, WS1). Her design showcased her sophisticated understanding of multi-layered digital threats and, at the same time, her simple approach to addressing these threats by pressing the button. Additionally, children often choose immediate disconnection as a response to privacy risks. Strategies included turning off devices, unplugging them, or disconnecting the Internet or intruders, which they perceived as sufficient measures to regain control. For example, Emma designed a button to eliminate spammers and hackers (Figure 3A), while Lily envisioned a robot that would delete scammers automatically (Figure 3D). Children also preferred the interaction they were familiar with, like mouse and clicking. Leo designed a computer mouse-like device with standard functions such as left-click, right-click, and scroll, alongside a dedicated "disconnect" button. He explained, "*If you press the disconnect button and there are no hackers, you'll just do nothing... sometimes it'll give you a message saying there are no hackers to disconnect*" (Leo, 9, M, DS5, WS1).

Unlike their desire to learn about privacy management skills and their sophisticated strategies, children's privacy protection strategies when facing potential privacy risks remained straightforward and focused on eliminating the threats. This comparison suggested a critical gap in children's privacy literacy development - how can children's ability to turn their privacy management skills into effective privacy protection strategies be better supported? We will discuss this point in detail in Section 5.

4.4 Children's Privacy Learning Process: Internalizing Privacy Knowledge

Internalization refers to how children absorb privacy knowledge and apply it independently. Rather than focusing on "what" they learn, internalization is closely related to "how" they learn and what the process looks like. In our study, we observed three key steps during children's internalization of privacy knowledge, including establishing privacy autonomy, translating privacy knowledge into concrete designs, and adapting their strategies to different contexts. We present the details below.

4.4.1 Establishing Autonomy in Privacy. The children in the study generally started their internalization by establishing autonomy in privacy, meaning that they tried to make privacy personal. Establishing autonomy means that children understand privacy concerns are relevant to themselves and recognize the need to control their privacy. This autonomy serves as a key motivator in children's privacy learning. We observed the following three strategies that the children used to establish autonomy.

Foster Ownership of Privacy. Having a sense of ownership is the first step in fostering autonomy of privacy. In DS1, when discussing privacy, children often used terms like "my," "your," and "our" to highlight personal control over spaces and belongings. For example, when asked about privacy in their daily lives, most children mentioned their rooms first. Lucas remarked, "*It is your room,*" (Lucas, 6, M, DS2, WS1) while Ethan added, "*It is his room, he owns it*" (Ethan, 7, M, DS1, WS1). As the workshop progressed, we also noted children's increasing usage of the terms "my" and "our" to emphasize their privacy widely. In DS1 of both workshops, children only used these terms to discuss what privacy is, then in DS2, children started to use the same terms to refer to their personal boundaries. For example, Emma used "*my privacy*" when she did not want to share her drawings with others. They also used "*that's our privacy*" when they found the cameras. Furthermore, in DS2 of the first workshop, Emma, Ethan, Grace, and Mia built a privacy space using removable whiteboards and desks (Figure 4). They described it as "***our** privacy space.*" From DS3, they frequently referred to this personal space as "*our privacy space*" and refused others to enter these spaces. During the workshop, children increasingly recognized and asserted ownership of their privacy, reflecting a growing sense of control over their privacy and boundaries.

Establish a Sense of Privacy from Everyday Objects. As an abstract concept, privacy can be difficult for children to understand. In our study, all children's understanding of privacy started with items or objects that they were familiar with in their daily lives, such as their houses or their rooms. Oftentimes, some children also used analogies as a medium to understand privacy. For example, when we discussed the information flow behind Amazon Echo, Leo provided an analogy to help his little brother understand the concept of information and hackers, "*The information is in a store, and hackers are like thieves*" (Leo, 9, M, DS3, WS1). By mapping the concepts of information and hackers to a story and thieves, respectively, Leo was able to summarize a fairly accurate understanding of privacy.

Another related trend we observed is that children initially focused on visible, physical objects, such as cameras and private rooms, before expanding their thoughts to more abstract objects, such as online accounts and passwords. For example, when discussing how to mitigate privacy risks for Amazon Echo, children in both workshops consistently suggested blocking the cameras before considering other options, such as changing privacy settings, switching accounts, and limiting device access.

Mixing Privacy and Safety. When discussing privacy, children naturally mixed the concept of privacy with safety. They reacted strongly to the potential negative consequences of their safety, such as being scammed, hacked, or losing money. For instance, when asked who might be interested in the information Amazon Echo collected, the children listed several threats, including hackers, scammers, and kidnappers. Emma said, "*Maybe hackers, robbers, or kidnappers*" (Emma, 9, F, DS2, WS1), and Mia added, "*Also criminals, evil people, cutters*" (Mia, 10, F, DS2, WS2). Emma added further, "*Bad people could use that information to hack you, rob you, or even kidnap you*" (Emma, 9, F, DS2, WS1). This concern for personal safety strongly influenced their approach to designing privacy protections. Many children focused on eliminating safety threats. For example, Leo designed a shotgun to prevent intruders from unlocking his personal items, while Lily envisioned a robot capable of deleting scammers (Figure 3D). Parents also reinforced these concerns. In DS5, James's mother highlighted the financial risks by emphasizing "bank accounts lost, money lost" as part of their design, drawing attention to the broader security implications associated with privacy (Figure 3B-iii).

4.4.2 Translate Knowledge into Concrete Designs. Another key step for children's privacy learning is to translate their knowledge into concrete designs. In the study, we focused on understanding how the children's knowledge influences their design process and the design outcomes, their thought process, and how their approaches evolved across different design sessions. We found that in each design session, children were able to reflect on their designs from previous days, identify new privacy issues, and come up with new solutions to mitigate those issues.

For example, as the workshops progressed, we observed how the children began to put their understanding of privacy into practice, particularly during break times when they were free to play. In DS1, after discussing the concept of privacy, some children created a "privacy space," setting rules such as verifying who had access. As Figure 4A, B show, they set a small entrance to control the access of the "privacy space". This process demonstrated how they started to translate the discussions around privacy into practical actions, reinforcing their ability to control access to their personal spaces. By DS2, three children had controlled the "privacy space" in our lab together. They have established clear boundaries and refused others to enter without their permission (Figure 4). In DS3, they further implemented new controls for the "privacy space" by setting a password for entry and designating a single entrance for easier management (Figure 4A, B). They treated this physical space as containing "private information," enforcing the use of the password for anyone wanting to enter or exit. To safeguard the space, they also volunteered to take turns as security guards (Figure 4C, D, E) and set clear rules, such as not sharing the password with others.

Interestingly, they also demonstrated evolving strategies to handle different situations. For example, in DS3, after giving one researcher the password and allowing them to enter their "privacy space", the children demonstrated thoughtful consideration when the researcher requested to take a photo of their whiteboard. Before agreeing to the request, the children asked who else could access the photo. After receiving a satisfactory explanation, the children gave the researcher permission to continue recording.

The constant reflection also allows the children to discover new privacy issues that were not noticed previously, as illustrated by children's attitude toward camera usage during the design workshops[5]. At the start of the workshop in DS1, children were informed of the camera recording as part of our data collection. None of the children questioned the presence of the cameras. After the discussion around privacy and the design activities in DS1, at the beginning of DS2, some children immediately noticed the camera usage. They reacted by saying, "*Hey, it's our privacy!*" and inquired about the purpose of the cameras. We explained the purpose of our data collection and why it was necessary for the research, then obtained their consent again before we continued the session. The two examples showed children become curious about the contexts in

[5]The camera is owned by our lab and is used for collecting video and audio data, as we discussed in the Method section.

which privacy resides and make privacy decisions based on actively sought information.

These voluntary progressions in children's privacy knowledge, awareness, and ability to take action showed how children were able to reflect on the discussion and design activities in the workshop and act accordingly based on their reflections. This *reflection and action* process has been observed among multiple children in both design workshops, suggesting a consistent pattern in children's privacy learning. We will further unpack this point in the Discussion 5.2.

4.4.3 Develop Context-Based Privacy Skills. As the workshop progressed, children showed an increasing ability to differentiate between various privacy contexts, indicating a context-based understanding of privacy. We also observed several factors that the children used to assess the contexts, including timing, stakeholders, and the nature of information.

Timing. Children appeared to assess the context and the privacy issues based on timing. Initially, when they focused on physical privacy, they used timing to determine what was considered private. For instance, Emma emphasized that her room felt private when she was out while Mia noted that her room was private only at specific times of the day, not at night or early morning. James highlighted the bathroom as a private space, "*especially when occupied*" (James, 11, M, DS1, WS2). After the children engaged in more discussions, they used timing to assess the privacy situation of their digital privacy. For example, Lily mentioned, "*Because Alexa can listen at any time. So if you're talking about something private, I normally close it*" (Lily, 10, F, DS1, WS2). Similarly, Henry, Chloe, and Jack proposed time-based controls to protect privacy when using smart home devices, such as turning them off when sleeping or away.

Stakeholders. Another factor that the children considered when assessing the privacy situation relates to the stakeholders that were involved in the situation. They expressed a high level of trust in family members, such as parents and siblings, and were comfortable sharing their personal information with them. As discussed in Section 4.1.2, their trust also extended to teachers who they believed would handle their privacy responsibly. Additionally, the children clearly differentiated sharing information with those they trust (e.g., family members and friends) from strangers. Emma emphasized this, saying, "*Why do I keep a password secret from my family members? But it's obvious for strangers*" (Emma, 9, F, DS1, WS1). This distinction between trusted and untrusted individuals was also critical for some children when assessing privacy situations online. James stated, "*Don't trust anyone online,*" (James, 11, M, DS3, WS2) while Lily warned against trusting gamers and scammers, saying, "*They can take your info*" (Lily, 10, F, DS3, WS2).

Some children considered the stakeholder the only key factor that affected their privacy decisions. For example, Chloe designed a simulation game in which children would try to separate the "good" players from the "bad" ones and decide with whom to share their information. In this game, the "bad" ones represented those who may access their personal information in their real lives. This consideration of the involved stakeholder also extends to commercial privacy. While they generally trusted companies like Amazon, they were more cautious about potential threats from hackers, scammers, and kidnappers. For example, James created a color-based visualization to show where his data went when he used social media, where blue represented trust in Amazon, yellow indicated moderate risk for advertisers, and red signified high risk for malicious actors like hackers and scammers (Figure 3B).

As mentioned in Section 4.4.1, children asked for more information when they needed to make privacy decisions, such as the recording of the workshops and photos of their drawings in their "privacy space". In their inquiries, they focused on asking who would have access to this information. For example, Emma and Mia asked "*who else could see them but you? Your boss? Your mentor?*" (Emma, 9, F, DS3, WS1). Upon learning that only trained and approved researchers in our lab could view them and that they would not be leaked, they permitted us to photograph their drawings in their "privacy space."

Nature of Information. Besides the previous two factors, children also considered the nature of the collected data as a factor when assessing the privacy situation. Children developed a hierarchy of information to navigate privacy across different contexts, shaped by factors such as the physical environment, perceived risk, and their willingness to share. For instance, Lily and most of the children were comfortable with security cameras outside their homes for monitoring intruders but opposed indoor cameras. They suggested that indoor cameras collected information about their families, which they considered private, demonstrating a clear boundary between public and private spaces. Henry suggested placing Amazon Echo in the living room rather than the bedroom, underscoring his concerns about his activities in the bedroom. Children's designs also reflected their consideration of the nature of collected information. For instance, Lily designed a device to show her the information flow behind Amazon Echo. This device would use blue for less critical information, yellow for moderately important data, and red for highly sensitive information—so sensitive and private that even family members might not be aware of it.

5 Discussion

5.1 Children's Needs and Expectations for Privacy Controls

The design activities allowed us to closely study children's privacy needs and their expectations of privacy controls in different technological contexts. We noticed children's distinct concerns and ways to protect their privacy which were tied to the specific features and risks of each type of technology or device.

Smart Home Devices. Children emphasized the need for robust control mechanisms to manage real-time data collection by smart home devices, particularly cameras, and microphones, as highlighted in Section 4.2.3, Section 4.4.1, and Section 4.4.2. They preferred physical privacy controls (e.g., camera covers and mute buttons) over digital options (e.g., in-app settings), citing the clarity and immediacy of physical tools. Additionally, they stressed the importance of determining the physical placement of these devices to better control data collection within private spaces. These expectations reflect their need to prioritize tangible, user-friendly controls to maintain privacy in shared, familial environments where these technologies operate continuously.

Account Protection. When discussing online account protection, children emphasized the importance of having robust control over account login and access to protect their personal information

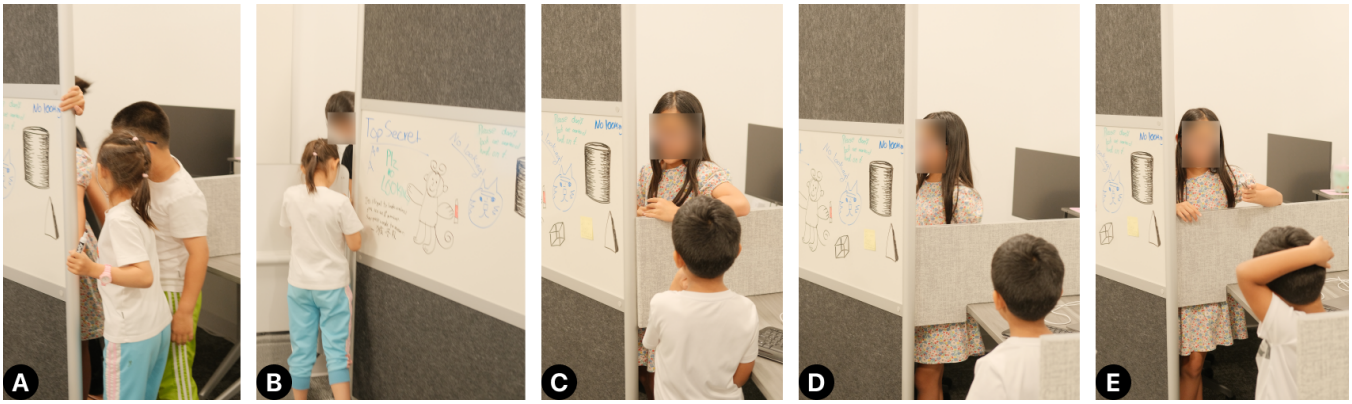

Figure 4: The "privacy space" activity involved children building a space. A. Children with permission to enter used the designated entrance to access the "privacy space." B. Children with permission exited the space through the designated exit. C. A child without access attempted to enter the "privacy space." D. The child assigned as the security guard asked for the password to allow entry into the "privacy space." E. The security guard child refused entry to the child after they failed to provide the correct password.

and prevent unauthorized use. They expressed a strong preference for multi-step authentication systems, particularly biometric authentication, as a unique and secure method for safeguarding accounts. These expectations, as discussed in Section 4.2.2, reflect their understanding of account security as a vital aspect of privacy control, especially for technologies that require personal logins or store sensitive information.

Social Media Platforms. In Section 4.2.4 and Section 4.4.1, children discussed the importance of privacy control for they actively shared personal information, such as posts, messages, and photos, on social media platforms. They sought features that would enable them to establish clear and strong boundaries for online interactions, ensuring protection from strangers, scammers, and spam. To do this, the expected privacy control should have easily configurable settings to define different levels of access for various groups, such as family members, friends, and online strangers. These preferences demonstrated their desire for granular control over who could view or engage with their content, reflecting their need for tailored privacy management on social platforms.

Media Consumption. When engaging with media-focused technologies (e.g., watching videos, listening to music, using voice assistants for jokes or trivia), children desired to maintain control over personalized recommendations to align with their preferences. As discussed in Section 4.1.3, they expected their personal information to be primarily used for advertising purposes. These interactions were viewed as a lower priority for privacy control, reflecting their passive and entertainment-oriented nature, which they perceived as presenting minimal privacy risks.

5.2 From Knowledge to Practice: Children's Privacy Learning Process

The setup of our co-design workshop allowed us to observe how children internalized the privacy knowledge they learned in one context (i.e., smart homes) and translated their knowledge into privacy designs in a broader set of contexts (e.g., social media, short videos). We reflect on the process as their privacy learning process can inform the development of effective educational strategies. Specifically, our findings suggest two key steps in children's privacy learning process, i.e., *reflection* and *action*. In our study context, we define reflection as children's self-reflection process; we also define action as how the children approach their designs in the co-design sessions. These two steps are interconnected - the children self-reflected on their actions to gain new knowledge about privacy, then applied the new knowledge to inform their new designs, forming an iterative learning cycle. This iterative process highlights the importance of privacy learning through *experiences* rather than as a static concept.

To further characterize the connection between the two steps in children's privacy learning, we used Donald Schön's theory of *Reflection in Action* and *Reflection on Action* as a valuable lens to describe the learning process [64]. According to Schön, *Reflection in Action* refers to thinking about one's experience during an event—adjusting behaviors and decisions as the situation unfolds, whereas *Reflection on Action* refers to evaluating past interventions to improve future practices and preparing for future actions, often with guidance from mentors [64]. In our study context, reflection in action relates to children's self-reflection on their designs as they were designing them, while reflection on action refers to children's reflection on their designs during their debriefs and presentations.

Reflection in Action: Reflection on Immediate Decision-Making. Children in our study frequently engaged in reflection in action as the privacy problems started to unfold and they were working on new designs to mitigate these privacy issues. For example, in DS2 of the first workshop, when children interacted with the Amazon Echo, they initially just explored it casually, but soon, three children independently discovered the physical camera blocker feature and turned it off. With this experience, when we asked the children to design a feature to help them mitigate the privacy issues in Amazon Echo, they immediately began brainstorming solutions like using one-way mirrors or creating covers for the device. This immediate reflection suggested children's "reflection

in action" skills - consideration for privacy organically appeared as they explored the device, urging them to make privacy designs on the spot to address their concerns. Such reflections, however, tend to remain at the surface level and are not comprehensive, mostly because the children may not have the required skills and guidance to reflect on things beyond the immediate privacy problems, such as the cause of the privacy problems and the long-term consequences of their privacy designs.

Reflection on Action: Reflection on Past Privacy Decisions. The other type of reflection relates to children's reflection on action. In our study context, the children would reflect on the designs they made during the activities through group discussions and presentations, during which they revisited their designs, collected feedback from others, and thought critically about how they might design differently. The children would iterate their original designs based on the outcomes of such reflections, or take the reflection into consideration when they designed new privacy mechanisms for the next day's co-design sessions. For instance, after designing privacy controls for smart homes, some children realized they lacked knowledge about certain privacy threats or the stakeholders involved in data collection, allowing us to offer more targeted and, arguably, more engaging privacy education to children. The increased knowledge would help the children refine their understanding of privacy and, in turn, influence how children adopt new privacy solutions.

Such reflections go beyond the surface level and help children establish a deeper understanding of the complexities of privacy management, prompting them to ask questions such as, "Who can see my data, and what are they doing with it?" Thus, this reflect-on-action process is crucial for fostering autonomy in children's privacy literacy development.

5.3 Support Reflection and Action in Children's Privacy Learning

The essence of reflection and action in children's privacy learning, from our perspective, is to realize that this is a long-term, iterative process that requires support from different aspects. In this section, rooted in our results, we discuss the elements that we deem important in supporting children's reflection and action in their privacy learning process.

5.3.1 Beyond Digital Interfaces: Tangible Designs to Facilitate Easy Reflection. Our findings showed that children often grasped the concept of privacy by mapping them to physical privacy concepts that they are familiar with, such as their home, bathrooms, or other types of personal spaces (Section 4.1.1). These results are in line with the findings from prior work where children connected the abstract concept of privacy with physical, private objects, such as potty [48]. When the children debriefed their understandings in the workshop, they were able to reflect on such understandings and translate them into concrete, physical design ideas, from which we could easily see the impact of such analogies, such as the one-way mirrors (e.g., "*I can see Alexa, but it can't see me*") and shells, covers, or boxes for Amazon Echo to prevent data collection, etc. Similarly, other designs, such as a physical representation of this process of social media from James and a robot incorporated physical indicators to inform users about "*what is true and not true online*" from Henry, also reflected children's inclination to engage with privacy through embodied and tangible methods.

Embodied learning is an educational approach that emphasizes the body's role in the learning process. It has proven effective in teaching abstract concepts, like AI and digital literacy [26, 41], due to its flexible content delivery [28, 75] and diverse forms [15, 38]. Compared to traditional privacy education methods, such as e-books and games, embodied learning offers experiential opportunities that promote self-autonomy and reflection in a sensory-immersive environment, minimizing real-life privacy risks [11, 60].

5.3.2 Beyond the Research Lab: Risk-Free Simulation Environment to Support Reflection and Action. In our study, we observed children's increasing knowledge of privacy and their ability to translate their knowledge into concrete design ideas, mostly for hypothetical scenarios. For ethical and logistic reasons, we did not incorporate real-world privacy incident cases in the study. The children in the study also have not encountered major privacy incidents in their lives. Consequently, their understanding of managing such situations remains theoretical, as they lacked practical experience to reflect upon and learn from. As prior works showed, theoretical knowledge alone cannot guide children to make informed privacy decisions in their real lives [32, 56].

On the other hand, children's designs suggested their need for a risk-free environment that provides them with real-life experiences so that they can practice and continue to reflect on their knowledge and privacy skills. Chloe's privacy simulation game, where children faced the consequences for sharing information with "bad guys," points to the possibility of a privacy simulator or sandbox. For example, Chen et al. proposed an empathy-based sandbox approach that allows users to explore the connection between personal data and the advertisement they see [10]. We envision a similar, hands-on approach that allows children to practice making privacy-related decisions in a controlled, risk-free environment. For example, we imagine a sandbox in which children are presented with various scenarios in which they need to make privacy decisions. When they make a decision, the sandbox will provide children with immediate feedback. This is crucial because it not only reinforces the impact of their privacy decisions but also offers an opportunity for "reflection in action." Children in our study expressed a strong preference for real-time notifications and previews about their privacy. For example, after changing the sharing preferences on a platform, they should receive an instant visual representation of what information becomes visible to others. This direct feedback helps children understand the consequences of their actions, promoting better privacy management over time.

We believe that such simulation-based approaches can offer valuable opportunities for children to develop risk assessment and decision-making skills, making privacy learning experiences more impactful and engaging.

5.3.3 Beyond Singular Learning Support: Use Multiple Learning Sources to Complement Reflection. In our study, we noticed children's reflection on their right to know the big picture about their privacy and the stakeholders involved in addition to privacy concepts (e.g., Section 4.2.1). This trend is reflected in their design ideas. For instance, Ethan designed a website that provides privacy-related knowledge, while Emma's design visualized information

transfer that includes multiple stakeholders in the Amazon Echo ecosystem. Similarly, Leo expressed a strong desire to understand more about the stakeholders who may access and be interested in his data. This desire for a broader understanding mirrors trends in other technological literacy, such as algorithmic literacy [79].

Yet, addressing this need requires support from multiple sources (e.g., teachers, parents, communities) so that they can complement each other. Existing research has already called for joint efforts to enhance children's privacy education, recognizing that long-term and multi-angle scaffolding is crucial [35, 66]. For example, Livingstone highlights the importance of a comprehensive system that involves parents, educators, and child support workers to develop children's privacy literacy [66]. Such collaborative effort not only provides sustained support but also helps children think about privacy from multiple angles.

Privacy decisions are made within complex contexts involving various stakeholders. As children grow older, they will need to navigate privacy conflicts, including those with family members [24, 29]. In our study, younger children generally trusted their parents with privacy matters, but literature indicates that this trust may evolve into tension as children mature. Privacy education must therefore help children manage these dynamics and develop awareness of institutional privacy practices.

5.3.4 Beyond Privacy Knowledge: Support Privacy Management and Privacy Control. In children's designs, we found a distinction between children's approaches to privacy management and privacy protection. Although similar, the children considered privacy management as an ongoing, proactive process in their daily lives, and privacy protection as a defensive response when actual privacy threats happen, each of which has different implications for children's reflection and action process.

Proactive Privacy Management. Throughout the co-design workshops, the children developed a sense of privacy management that involved actively controlling who can access personal information and how that information is shared. As a result, privacy management tools primarily increased children's situational awareness about privacy so that they could make informed privacy decisions. For example, Ethan's 3D model visualized data flow to show where his information was going, while James's data flow visualization offered a real-time overview of information flow on social media. These designs reflect children's understanding that managing privacy is an ongoing process that requires constant attention, providing a way for children to implement "*reflection on action*."

Reactive Privacy Control. In contrast, protecting privacy was often framed as a more reactive process, focused on safeguarding against specific threats. For instance, children frequently connected privacy with personal safety, linking it to concerns such as being kidnapped or losing money. This defensive approach to privacy reflected their desire to shield themselves from harm, particularly when they felt vulnerable. Children's protective instincts were most evident when they discussed and designed for specific privacy incidents. For example, when asked to think about the consequences of privacy violations, they quickly raised concerns about the risks of sharing personal information online, suggesting that their protective instincts were triggered when they perceived an immediate danger, creating an opportunity for "*reflection in action*."

5.4 Implications for Child-friendly Privacy Designs

In addition to insights that support children's privacy learning, we also drew implications for children-friendly privacy designs based on the co-design outcomes from our study.

5.4.1 Age-Appropriate Privacy Languages and Elements. Like other information provided to children [79], privacy language should match children's cognitive levels, avoiding technical jargon or legal terms. For example, Leo's information is in a store and hackers are like thieves. Chloe used "good guys" and "bad guys" to represent parties involved in the data process, and she also used "secrets" to make privacy easy for other children to understand. Instead of "data collection" or "third-party access," terms like "your information" or "people you don't know" can make privacy more relatable and easier to understand. Additionally, children's approaches to privacy are heavily shaped by visual metaphors, such as the color-coded privacy indicators (red for "public" and green for "private") on the robot and one-side mirror to block the camera on Amazon Echo. Thus, when communicating with children about privacy-related information (e.g., display digital warning messages which were often ignored [40]), designers can make the abstract concept of privacy more comprehensible for children by using age-appropriate privacy languages and design elements.

5.4.2 Autonomy-based Framing. According to the third-person effect theory [16], children may believe privacy risks affect others more than themselves [17], limiting their critical thinking about privacy. To address this, privacy language should emphasize personal relevance and autonomy. Asset-based framing encourages children to see privacy as something they can control, rather than a vulnerability [82]. By building on their existing knowledge and mental models, such as linking privacy with personal safety (e.g., avoiding being hacked or losing money), children feel more empowered to manage their own privacy. This approach promotes autonomy by treating privacy as an active part of their everyday lives. Highlighting both positive and negative consequences of privacy decisions helps make abstract risks more understandable [30, 31, 92]. In our study, children responded more strongly to threats, like being hacked or losing data, when they were shown concrete outcomes. Thus, we suggest using clear, relatable scenarios to illustrate these consequences to help children understand the risks and benefits of privacy decisions. Incorporating asset-based framing and demonstrating consequences can foster deeper understanding and encourage children to take ownership of their privacy decisions.

5.4.3 Guided Privacy Choice. Currently, technologies targeting ages 13 and older are attempting to design toward more user-friendly privacy notice and choice [23, 63]. However, we did not observe a similar trend for privacy choices in technologies that target younger children, suggesting the need to support young children's privacy decision-making [88].

We suggest that privacy choice interfaces should include guided assistance. Prompts and context-specific questions embedded within

privacy options (e.g., "Would you like to share this content with everyone or just friends?") can encourage children to think critically about their choices. These design elements provide scaffolding for children as they navigate complex privacy decisions, fostering independent and informed thinking about their digital privacy.

6 Future Work

Our study highlights several opportunities for future research in children's privacy education and technology design. First, while we explored how children internalize privacy knowledge through co-design activities, further longitudinal studies are necessary to examine how these privacy practices evolve over time. Observing children's behaviors and privacy decision-making as they mature would provide valuable insights into the long-term effectiveness of co-design approaches in fostering privacy literacy. Second, future work should explore diverse cultural and socio-economic contexts to understand how children's privacy needs and expectations differ. Our study focused on a specific demographic; expanding this to include children from various backgrounds will allow for a more comprehensive understanding of privacy challenges and design solutions that can be universally applied. Lastly, future research should involve deeper engagement with families, educators, developers, and policymakers to co-create privacy education frameworks that can be applied across formal and informal learning environments. Developing scalable models of co-design for privacy education, supported by stronger regulatory frameworks, can help ensure that children's privacy rights are upheld in increasingly complex digital ecosystems.

7 Conclusion

In the digital age, children are increasingly exposed to privacy risks as their data is continuously collected, tracked, and monetized. Despite efforts to educate children about privacy, there remains a gap in understanding how they apply this knowledge to their daily practices and what privacy controls they expect. This study addressed these gaps by conducting two five-day co-design workshops with 11 children aged 6-11 and their parents. Our findings revealed distinct variations in children's perceptions of privacy across interpersonal, institutional, and commercial contexts. We also identified a mismatch between children's advanced expectations for privacy management, such as robust authentication methods, and their actual practices, which often involve simpler measures like unplugging devices. Our paper made three significant contributions. First, we provided a nuanced understanding of children's expectations for privacy controls and their practical applications. Second, we extended existing research by exploring how children translate privacy knowledge into everyday practices, emphasizing the need for support systems that enhance their privacy literacy. Finally, we offered actionable design implications for creating child-friendly privacy designs that address these needs and expectations. These findings not only advance our understanding of children's privacy literacy but also inform the development of more effective privacy interventions and tools.

Acknowledgments

We thank the anonymous reviewers for their valuable feedback and all the children and parents for their participation. We also thank the valuable feedback from Zikai Alex Wen, Abijith Manikandan, Scott Spencer, and Sasha Holt. This work is in part supported by the National Science Foundation CNS-2426397, CNS-2232653, a Meta Research Award, and a Google PSS Faculty Award.

References

[1] Mamtaj Akter, Amy J. Godfrey, Jess Kropczynski, Heather R. Lipford, and Pamela J. Wisniewski. 2022. From Parental Control to Joint Family Oversight: Can Parents and Teens Manage Mobile Online Safety and Privacy as Equals? *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW1 (2022), 57:1–57:28. https://doi.org/10.1145/3512904

[2] Kenan Kamel A Alghythee, Adel Hrncic, Karthik Singh, Sumanth Kunisetty, Yaxing Yao, and Nikita Soni. 2024. Towards Understanding Family Privacy and Security Literacy Conversations at Home: Design Implications for Privacy Literacy Interfaces. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 983, 12 pages. https://doi.org/10.1145/3613904.3641962

[3] Noura Alomar and Serge Egelman. 2022. Developers Say the Darnedest Things: Privacy Compliance Processes Followed by Developers of Child-Directed Apps. *Proceedings on Privacy Enhancing Technologies* 2022 (10 2022), 250–273. https://doi.org/10.56553/popets-2022-0108

[4] Karla Badillo-Urquiola, Diva Smriti, Brenna McNally, Evan Golub, Elizabeth Bonsignore, and Pamela J. Wisniewski. 2019. Stranger Danger! Social Media App Features Co-designed with Children to Keep Them Safe Online. In *Proceedings of the 18th ACM International Conference on Interaction Design and Children (IDC '19)*. Association for Computing Machinery, New York, NY, USA, 394–406. https://doi.org/10.1145/3311927.3323133

[5] Mathilde Bekker, Julie Beusmans, David Keyson, and Peter Lloyd. 2003. KidReporter: a user requirements gathering technique for designing with children. *Interacting with Computers* 15, 2 (04 2003), 187–202. https://doi.org/10.1016/S0953-5438(03)00007-9 arXiv:https://academic.oup.com/iwc/article-pdf/15/2/187/7800210/iwc15-0187.pdf

[6] Stacy Black, Rezvan Joshaghani, Dhanush kumar Ratakonda, Hoda Mehrpouyan, and Jerry Alan Fails. 2019. Anon what what? Children's Understanding of the Language of Privacy. In *Proceedings of the 18th ACM International Conference on Interaction Design and Children (IDC '19)*. Association for Computing Machinery, New York, NY, USA, 439–445. https://doi.org/10.1145/3311927.3325324

[7] Virginia Braun and Victoria Clarke. 2013. *Successful qualitative research: a practical guide for beginners*. SAGE, Los Angeles. OCLC: ocn811733656.

[8] Jasmina Byrne, Daniel Kardefelt-Winther, Sonia Livingstone, and Mariya Stoilova. 2016. *Global Kids Online research synthesis, 2015–2016.* Technical Report. UNICEF Office of Research– Innocenti and London School of Economics and Political Science, London, United Kingdom. http://globalkidsonline.net/synthesis-report/

[9] Cansu Caglar. 2021. Children's Right To Privacy And Data Protection: Does the Article on Conditions Applicable to Child's Consent Under the GDPR Tackle the Challenges of the Digital Era or Create Further Confusion? *European Journal of Law and Technology* 12, 2 (2021), 1–31.

[10] Chaoran Chen, Weijun Li, Wenxin Song, Yanfang Ye, Yaxing Yao, and Toby Jia-Jun Li. 2024. An Empathy-Based Sandbox Approach to Bridge the Privacy Gap among Attitudes, Goals, Knowledge, and Behaviors. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 234, 28 pages. https://doi.org/10.1145/3613904.3642363

[11] Jaewon Cho, Junwoo Yoo, Ju-young Shin, Jun-dong Cho, and Andrea Bianchi. 2017. Quantifying Children's Engagement with Educational Tangible Blocks. In *Proceedings of the Eleventh International Conference on Tangible, Embedded, and Embodied Interaction (TEI '17)*. Association for Computing Machinery, New York, NY, USA, 389–395. https://doi.org/10.1145/3024969.3025062

[12] Chhaya Chouhan, Christy M LaPerriere, Zaina Aljallad, Jess Kropczynski, Heather Lipford, and Pamela J Wisniewski. 2019. Co-designing for community oversight: Helping people make privacy and security decisions together. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–31.

[13] Ananta Chowdhury and Andrea Bunt. 2023. Co-Designing with Early Adolescents: Understanding Perceptions of and Design Considerations for Tech-Based Mediation Strategies that Promote Technology Disengagement. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, Hamburg Germany, 1–16. https://doi.org/10.1145/3544548.3581134

[14] Diane J. Cook. 2012. How Smart Is Your Home? *Science* 335, 6076 (2012), 1579–1581. https://doi.org/10.1126/science.1217640 arXiv:https://www.science.org/doi/pdf/10.1126/science.1217640

[15] Giulia Cosentino, Mirko Gelsomini, and Michail Giannakos. 2023. MOVES: Going beyond hardwired multisensory environments for children. In *Proceedings of the 22nd Annual ACM Interaction Design and Children Conference (IDC '23)*. Association for Computing Machinery, New York, NY, USA, 716–720. https://doi.org/10.1145/3585088.3594493

[16] W. Phillips Davison. 1983. The Third-Person Effect in Communication. *The Public Opinion Quarterly* 47, 1 (1983), 1–15. https://www.jstor.org/stable/2748702

[17] Bernhard Debatin, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes. 2009. Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication* 15, 1 (Oct. 2009), 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

[18] Nicola Dell, Vidya Vaidyanathan, Indrani Medhi, Edward Cutrell, and William Thies. 2012. "Yours is better!": participant response bias in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Austin, Texas, USA) *(CHI '12)*. Association for Computing Machinery, New York, NY, USA, 1321–1330. https://doi.org/10.1145/2207676.2208589

[19] 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 (March 2022), 100446. https://doi.org/10.1016/j.ijcci.2021.100446

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

[21] 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

[22] Anirudh Ekambaranathan, Jun Zhao, and Max Van Kleek. 2021. "Money makes the world go around": Identifying Barriers to Better Privacy in Children's Apps From Developers' Perspectives. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 46, 15 pages. https://doi.org/10.1145/3411764.3445599

[23] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 64, 16 pages. https://doi.org/10.1145/3411764.3445148

[24] 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

[25] Donell Holloway, Lelia Green, and Sonia Livingstone. 2013. . LSE, London.

[26] 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

[27] Patrick C. K. Hung, Farkhund Iqbal, Shih-Chia Huang, Mohammed Melaisi, and Kevin Pang. 2016. A Glance of Child's Play Privacy in Smart Toys. In *Cloud Computing and Security*, Xingming Sun, Alex Liu, Han-Chieh Chao, and Elisa Bertino (Eds.). Springer International Publishing, Cham, 217–231. https://doi.org/10.1007/978-3-319-48674-1_20

[28] Hyejin Im and Chris Rogers. 2021. Draw2Code: Low-Cost Tangible Programming for Creating AR Animations. In *Proceedings of the 20th Annual ACM Interaction Design and Children Conference (IDC '21)*. Association for Computing Machinery, New York, NY, USA, 427–432. https://doi.org/10.1145/3459990.3465189

[29] 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

[30] Bart Knijnenburg and David Cherry. 2016. Comics as a Medium for Privacy Notices. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 1–9. https://www.usenix.org/conference/soups2016/workshop-program/wfpn/presentation/knijnenburg

[31] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2017. 'No Telling Passcodes Out Because They're Private': Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 64:1–64:21. https://doi.org/10.1145/3134699

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

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

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

[35] Lanjing Liu, Lan Gao, Nikita Soni, and Yaxing Yao. 2024. Exploring Design Opportunities for Family-Based Privacy Education in Informal Learning Spaces. In *Proceedings on Privacy Enhancing Technologies*, Vol. 3. PoPETS, Bristol, UK, 127–143. https://doi.org/10.56553/popets-2024-0071

[36] Lanjing Liu, Lan Gao, and Yaxing Yao. 2024. Integrating Family Privacy Education and Informal Learning Spaces: Characteristics, Challenges and Design Opportunities. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA '24)*. Association for Computing Machinery, New York, NY, USA, Article 197, 9 pages. https://doi.org/10.1145/3613905.3650940

[37] Lanjing Liu, Chao Zhang, and Zhicong Lu. 2024. Wrist-bound Guanxi, Jiazu, and Kuolie: Unpacking Chinese Adolescent Smartwatch-Mediated Socialization. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 906, 21 pages. https://doi.org/10.1145/3613904.3642044

[38] Yu-Yu Liu and Ole Sejer Iversen. 2022. Computational Thinking through Tangible Play: Understanding Social Dialogues in Children's Learning. In *Proceedings of the 21st Annual ACM Interaction Design and Children Conference (IDC '22)*. Association for Computing Machinery, New York, NY, USA, 596–603. https://doi.org/10.1145/3501712.3535288

[39] Sonia Livingstone, Leslie Haddon, Anke Görzig, and Kjartan Ólafsson. 2011. *Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries*. Technical Report. EU Kids Online, The London School of Economics and Political Science.

[40] Sonia Livingstone and Amanda Third. 2017. Children and young people's rights in the digital age: An emerging agenda. *New Media & Society* 19, 5 (2017), 657–670. https://doi.org/10.1177/1461444816686318 arXiv:https://doi.org/10.1177/1461444816686318

[41] Duri Long, Mikhail Jacob, and Brian Magerko. 2019. Designing Co-Creative AI for Public Spaces. In *Proceedings of the 2019 on Creativity and Cognition (C&C '19)*. Association for Computing Machinery, New York, NY, USA, 271–284. https://doi.org/10.1145/3325480.3325504

[42] Mary Madden, Amanda Lenhart, Sandra Cortesi, and Urs Gasser. 2013. *Teens and Mobile Apps Privacy*. Technical Report. Pew Research Center.

[43] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy Attitudes of Smart Speaker Users. *Proceedings on Privacy Enhancing Technologies* 2019 (2019), 22. Issue 4. https://petsymposium.org/popets/2019/popets-2019-0068.php

[44] Giovanna Mascheroni and Donell Holloway. 2019. *The quantified child: Discourses and practices of dataveillance in different life stages*. Routledge, London, United Kingdom. 354–365 pages.

[45] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on human-computer interaction* 3, CSCW (2019), 1–23.

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

[47] Ingrida Milkaite, Ralf De Wolf, Eva Lievens, Tom De Leyn, and Marijn Martens. 2021. Children's reflections on privacy and the protection of their personal data: A child-centric approach to data protection information formats. *Children and Youth Services Review* 129 (Oct. 2021), 106170. https://doi.org/10.1016/j.childyouth.2021.106170

[48] Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Faith Cranor. 2018. Turtles, Locks, and Bathrooms: Understanding Mental Models of Privacy Through Illustration. In *Proceedings on Privacy Enhancing Technologies*, Vol. 2018. Proceedings on Privacy Enhancing Technologies, Barcelona, Spain, 5–32. Issue 4. https://doi.org/10.1515/popets-2018-0029

[49] U.S. Department of Health and Human Services. 2021. Preventing Cyberbullying in the Age of Smart Phones. Accessed: 2023-04-26.

[50] 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

[51] Anthony T. Pinter, Pamela J. Wisniewski, Heng Xu, Mary Beth Rosson, and Jack M. Caroll. 2017. Adolescent Online Safety: Moving Beyond Formative Evaluations to Designing Solutions for the Future. In *Proceedings of the 2017 Conference on Interaction Design and Children (IDC '17)*. Association for Computing Machinery, New York, NY, USA, 352–357. https://doi.org/10.1145/3078072.3079722

[52] Cristina Ponte. 2022. Datafied Childhoods: data practices and imaginaries in children's lives. *Journal of Children and Media* 16, 4 (2022), 613–616. https://doi.org/10.1080/17482798.2022.2124648 arXiv:https://doi.org/10.1080/17482798.2022.2124648

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

[54] Jenny S Radesky, Heidi M Weeks, Rosa Ball, Alexandria Schaller, Samantha Yeo, Joke Durnez, Matthew Tamayo-Rios, Mollie Epstein, Heather Kirkorian, Sarah Coyne, et al. 2020. Young children's use of smartphones and tablets. *Pediatrics* 146, 1 (2020), 1–8.

[55] 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

[56] Janet C. Read and Brendan Cassidy. 2012. Designing textual password systems for children. In *Proceedings of the 11th International Conference on Interaction Design and Children* (Bremen, Germany) *(IDC '12)*. Association for Computing Machinery, New York, NY, USA, 200–203. https://doi.org/10.1145/2307096.2307125

[57] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman. 2018. "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. In *Proceedings on Privacy Enhancing Technologies*, Vol. 2018. Proceedings on Privacy Enhancing Technologies, Barcelona, Spain, 63–83. https://doi.org/10.1515/popets-2018-0021

[58] V Rideout, A Peebles, S Mann, and MB Robb. 2022. Common Sense census: Media use by tweens and teens, 2021. Common Sense.

[59] Catherine Kohler Riessman. 2008. *Narrative methods for the human sciences*. Sage Publications, Inc, Thousand Oaks, CA, US.

[60] Lea Dujić Rodić and Andrina Granić. 2022. Tangible interfaces in early years' education: a systematic review. *Personal and Ubiquitous Computing* 26, 1 (Feb. 2022), 39–77. https://doi.org/10.1007/s00779-021-01556-x

[61] Elaheh Sanoubari, John Edison Muñoz Cardona, Hamza Mahdi, James E. Young, Andrew Houston, and Kerstin Dautenhahn. 2021. Robots, Bullies and Stories: A Remote Co-design Study with Children. In *Proceedings of the 20th Annual ACM Interaction Design and Children Conference (IDC '21)*. Association for Computing Machinery, New York, NY, USA, 171–182. https://doi.org/10.1145/3459990.3460725

[62] Benjamin Saunders, Julius Sim, Tom Kingstone, Shula Baker, Jackie Waterfield, Bernadette Bartlam, Heather Burroughs, and Clare Jinks. 2018. Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & Quantity* 52, 4 (July 2018), 1893–1907. https://doi.org/10.1007/s11135-017-0574-8

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

[64] Donald A. Schon. 1984. *The Reflective Practitioner: How Professionals Think In Action* (1st edition ed.). Basic Books, New York.

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

[66] Rishita Nandagiri Sonia Livingstone, Mariya Stoilova. 2019. *Children's data and privacy online: Growing up in a digital age. An evidence review.* London: London School of Economics and Political Science, London.

[67] Dan Su, Jiqiang Liu, Sencun Zhu, Xiaoyang Wang, and Wei Wang. 2020. "Are you home alone?" "Yes" Disclosing Security and Privacy Vulnerabilities in Alexa Skills. arXiv:2010.10788 [cs.CR] https://arxiv.org/abs/2010.10788

[68] Kaiwen Sun, Ritesh Kanchi, Frances Marie Tabio Ello, Li-Neishin Co, Mandy Wu, Susan A. Gelman, Jenny Radesky, Florian Schaub, and Jason Yip. 2024. "Why is Everything in the Cloud?": Co-Designing Visual Cues Representing Data Processes with Children. In *Proceedings of the 23rd Annual ACM Interaction Design and Children Conference* (Delft, Netherlands) *(IDC '24)*. Association for Computing Machinery, New York, NY, USA, 517–532. https://doi.org/10.1145/3628516.3655819

[69] Kaiwen Sun, Ritesh Kanchi, Frances Marie Tabio Ello, Li-Neishin Co, Mandy Wu, Susan A. Gelman, Jenny Radesky, Florian Schaub, and Jason Yip. 2024. "Why is Everything in the Cloud?": Co-Designing Visual Cues Representing Data Processes with Children. In *Proceedings of the 23rd Annual ACM Interaction Design and Children Conference* (Delft, Netherlands) *(IDC '24)*. Association for Computing Machinery, New York, NY, USA, 517–532. https://doi.org/10.1145/3628516.3655819

[70] Kaiwen Sun, Jingjie Li, Yixin Zou, Jenny Radesky, Christopher Brooks, and Florian Schaub. 2024. Unfulfilled Promises of Child Safety and Privacy: Portrayals and Use of Children in Smart Home Marketing. *Proc. ACM Hum.-Comput. Interact.* 8, CSCW1, Article 145 (apr 2024), 29 pages. https://doi.org/10.1145/3637422

[71] 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* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 687, 34 pages. https://doi.org/10.1145/3411764.3445333

[72] Kaiwen Sun, Yixin Zou, Jenny Radesky, Christopher Brooks, and Florian Schaub. 2021. Child Safety in the Smart Home: Parents' Perceptions, Needs, and Mitigation Strategies. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 471 (oct 2021), 41 pages. https://doi.org/10.1145/3479858

[73] Ruoxi Sun, Minhui Xue, Gareth Tyson, Shuo Wang, Seyit Camtepe, and Surya Nepal. 2023. Not Seen, Not Heard in the Digital World! Measuring Privacy Practices in Children's Apps. In *Proceedings of the ACM Web Conference 2023* (Austin, TX, USA) *(WWW '23)*. Association for Computing Machinery, New York, NY, USA, 2166–2177. https://doi.org/10.1145/3543507.3583327

[74] S S Tirumala, Abdolhossein Sarrafzadeh, and Paul Pang. 2016. A survey on internet usage and cybersecurity awareness in students. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, Auckland, New Zealand, 223–228. https://doi.org/10.1109/PST.2016.7906931

[75] Lorraine Underwood, Elizabeth Edwards, John Edward Vidler, Elisa Rubegni, and Joe Finney. 2023. Introducing Classroom Cloudlet: a mobile, tangible, and transparent approach to Internet of Things education. In *Proceedings of the 22nd Annual ACM Interaction Design and Children Conference (IDC '23)*. Association for Computing Machinery, New York, NY, USA, 740–744. https://doi.org/10.1145/3585088.3594487

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

[77] Maarten Van Mechelen, Alice Schut, Mathieu Gielen, and Remke Klapwijk. 2018. Developing children's empathy in co-design activities: a pilot case study. In *Proceedings of the 17th ACM Conference on Interaction Design and Children (IDC '18)*. Association for Computing Machinery, New York, NY, USA, 669–674. https://doi.org/10.1145/3202185.3210797

[78] Kellie Vella, Tshering Dema, Alessandro Soro, and Margot Brereton. 2022. Fostering Children's Stewardship of Local Nature Through Game Co-design. In *Proceedings of the 33rd Australian Conference on Human-Computer Interaction (OzCHI '21)*. Association for Computing Machinery, New York, NY, USA, 38–50. https://doi.org/10.1145/3520495.3522702

[79] Ge Wang, Jun Zhao, Max Van Kleek, and Nigel Shadbolt. 2023. 'Treat me as your friend, not a number in your database': Co-designing with Children to Cope with Datafication Online. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, Hamburg Germany, 1–21. https://doi.org/10.1145/3544548.3580933

[80] Cara Wilson, Margot Brereton, Bernd Ploderer, and Laurianne Sitbon. 2019. Co-Design Beyond Words: 'Moments of Interaction' with Minimally-Verbal Children on the Autism Spectrum. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3290605.3300251

[81] Christina L. Wissinger. 2017. Privacy Literacy: From Theory to Practice. *Communications in Information Literacy* 11, 2 (2017), 378–389. https://eric.ed.gov/?id=EJ1166461 ERIC Number: EJ1166461.

[82] Marisol Wong-Villacres, Aakash Gautam, Wendy Roldan, Lucy Pei, Jessa Dickinson, Azra Ismail, Betsy DiSalvo, Neha Kumar, Tammy Clegg, Sheena Erete, Emily Roden, Nithya Sambasivan, and Jason Yip. 2020. From Needs to Strengths: Operationalizing an Assets-Based Design of Technology. In *Companion Publication of the 2020 Conference on Computer Supported Cooperative Work and Social Computing* (Virtual Event, USA) *(CSCW '20 Companion)*. Association for Computing Machinery, New York, NY, USA, 527–535. https://doi.org/10.1145/3406865.3418594

[83] Julia Woodward, Zari McFadden, Nicole Shiver, Amir Ben-hayon, Jason C. Yip, and Lisa Anthony. 2018. Using Co-Design to Examine How Children Conceptualize Intelligent Interfaces. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3174149

[84] 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

[85] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy perceptions and designs of bystanders in smart homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–24.

[86] 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

[87] Jason C. Yip, Frances Marie Tabio Ello, Fumi Tsukiyama, Atharv Wairagade, and June Ahn. 2023. "Money shouldn't be money!" : An Examination of Financial Literacy and Technology for Children Through Co-Design. In *Proceedings of the 22nd Annual ACM Interaction Design and Children Conference (IDC '23)*. Association for Computing Machinery, New York, NY, USA, 82–93.

https://doi.org/10.1145/3585088.3589355

[88] Jason C. Yip, Kiley Sobel, Xin Gao, Allison Marie Hishikawa, Alexis Lim, Laura Meng, Romaine Flor Ofiana, Justin Park, and Alexis Hiniker. 2019. Laughing is Scary, but Farting is Cute: A Conceptual Model of Children's Perspectives of Creepy Technologies. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3290605.3300303

[89] 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

[90] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 65–80. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

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

[92] Leah Zhang-Kennedy, Khadija Baig, and Sonia Chiasson. 2017. Engaging children about online privacy through storytelling in an interactive comic. In *Proceedings of the 31st British Computer Society Human Computer Interaction Conference* (Sunderland, UK) *(HCI '17)*. BCS Learning & Development Ltd., Swindon, GBR, Article 45, 11 pages. https://doi.org/10.14236/ewic/HCI2017.45

[93] 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

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

[95] Fangwei Zhao, Serge Egelman, Heidi Weeks, Niko Kaciroti, Alison Miller, and Jenny Radesky. 2020. Data Collection Practices of Mobile Applications Played by Preschool-Aged Children. *JAMA pediatrics* 174 (09 2020), e203345. https://doi.org/10.1001/jamapediatrics.2020.3345

[96] 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

[97] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 200 (Nov. 2018), 20 pages. https://doi.org/10.1145/3274469

A Appendix

Table 2: The Codebook

Themes	Codes	Quotations
Interpersonal Privacy	Understanding of interpersonal privacy	They (parents) check my iPad everything, they have my password.
	Invade someone's privacy	Every time my family tries not to let me know what their passwords are... Sometimes I figured them out from older passwords, and they forget they're trying to keep the passwords away from me and accidentally say that while I asked them the passwords. My dad's computer, he said ****.
Institutional Privacy	Understanding of institutional privacy	They (Chromebooks) know my name, my age, my last name, probably they know more ... I'm OK with it.
	Blind trust in institutions	Because you are the teacher, from the university.
Commercial Privacy	Understanding of commercial privacy	So then they can sell the information to Spam also. And then Spam will call you.
	Misunderstanding of commercial privacy	RA: Who collects the boy's data? Jack: Google!
Establishing Autonomy in Privacy	Ownership	It is "his" room, he owns it.
	Start from everyday objects	Information is in a store, and hackers are like thieves.
	Mix privacy and safety	Because they (bad people) know how to hack you, rob you, what you like to bribe you so they can kidnap you.
	Control access	Filed notes: kids set a tiny entrance for their "privacy space".
Translate Knowledge into Concrete Designs	Judge the timing	Because Alexa can listen at any time. So if you're talking about something private, I normally close it.
	Judge the stakeholders	Who else could see them but you? Your boss? Your mentor? Are you sure?
	Judge the type of information	I am ok with that area (point the outside of a house). But in my bedroom, no!
Develop Context-Based Privacy Skills	Judge the timing	Because Alexa can listen at any time. So if you're talking about something private, I normally close it.
	Judge the stakeholders	Who else could see them but you? Your boss? Your mentor? Are you sure?
	Judge the type of information	I am ok with that area (point the outside of a house). But in my bedroom, no!
The Way They Want to Learn	Simulation	It's like a fish spam simulator. So there's this AI-generated spam and you practice how to get rid of it. That way, when you get actual spam, you know how to get rid of it.
	Gamification	I made a game to help kids with awareness of not just giving information away to like anybody. So basically it's a game that you can play. All the rules are here, but basically you have a five-minute timer and there's a bowl that you pick out of, and you're either trying to steal some of the information that the other people have or you're trying to just know the information. And you make up a fake secret like my phone number is 552.
Stay Aware	Know the data flow	This red box is like a scammer. Yellow equals advertisers and blue equals the database. The line means some information flow and the type of information.
	Know the principle behind	Who else could see them but you? Your boss? Your mentor? Are you sure?
	Record and report	You have to take photos and then install them in.
Authentication	Adaptive authentication	But it does if something does go wrong, it will destroy all code and make fresh new ones.
	Biometric authentication	I have a tail print. Like a fingerprint, but with a tail.
	Multiple authentications	This should be a wire that you plug in. You also plug it into the lock, and then you go to upload tail print, and then you click upload tail print and you put your tail print on the circle that says p short for tail print. This scoring shows upload tail print, it's loaded, and it's 80%. Once it's 100%, it's loaded and you can use your tail print to unlock it. You have to go through the three stages.
Minimal Privacy Exposure	Control information collection	Filed notes: Ethan asked for other kids if he could turn off the camera by the camera cover.
	Physical management	This is the camera, and these are the covers, so he can't really see us and listen to us.
	Reduce exposure	Don't expose any private information. Don't make an account. Try to just don't really go to the comment section if you want to be safe.

To be continued

Continued from the previous page

Themes	Codes	Quotations
Real-Time and Contextual Assistance	Offer tips	I just designed a tips board so people get to know, like, tips about not getting scammed accidentally.
	Contextual assistant	You can ask it if like, on the computer it says something, then you can ask if like what the computer says is true. It will answer.
Sense of Security	Feel be protected	The design will be used when you are hacked or scammed, bugs, and more are found or detected. The button can change and reset passwords, hackers, et.
Threat Detection and Understandable Feedback	Identify threats	Whenever the suspicious lock turns and, like, photographs a stranger and then makes him suspicious and then posts it into a wanted poster.
	Understandable Feedback	But a warning that will say that you are at least trying- you are getting hacked. So then you can just press- and if you like left click or right click then you press this button and beep.
Easy to handle	Disconnection	I like to plug it in case like Alexa usually you turn her off, she still listens.
	Remove the threat/threat maker	When you press the button, Jams, viruses, and no 100-meter radius

Table 3: The Protocol of Design Sessions

Session	Design Questions / Project Goals	Design Activities and Technique
Design Session 1	Set up children's role as designers Understand privacy awareness and management	**Throwing the Ball:** Start with a warm-up game to help children get to know each other and introduce the topic. As they catch the ball, invite them to share their answers to questions related to the privacy topic. **Focus Group:** Introduce the concept of privacy through warm-up questions and discussions of different privacy contexts, followed by exploring scenarios related to interpersonal, institutional, and commercial privacy. Warm-up questions vary depending on the group. **Design Task:** Design a new door lock for your privacy. Children start by sketching their design ideas on paper and then create design prototypes using DIY materials. **Show & Feedback:** Children present their designs and give each other feedback.
Design Session 2	Learn about children's privacy issues in their daily lives and how children control their privacy in their everyday lives.	**Play with Alex:** Children interact with an Echo device for 15 minutes while researchers observe potential privacy risks. Then we encourage children to reflect on their experiences. **Big Board:** The Big Board guides children in reflecting on privacy issues during their interactions, prompting them to consider what they said to the device, the information it may have collected, who might access it, and who could have an interest in it. **Brainstorming:** Encourage children to reflect on their experiences and think creatively. **Helping Hand:** Present a scenario where friends need help because they are unfamiliar with social media and smart home devices and are concerned about privacy. Encourage children to consider the potential privacy risks and practical strategies to protect privacy while using technology. **Design Task:** Create ideas for protecting privacy with smart home devices. Children start by sketching their design ideas on paper and then create design prototypes using DIY materials. **Showing Time:** Children present their designs and give each other feedback.
Design Session 3	Explore privacy beyond individual users and expand children's understanding through games and prototypes.	**Information Game:** Introduce how information flows when interacting with technology through a role-playing game (as Figure 5 shows). **Prototype:** Engage with a prototype to explore the information flow behind smart home devices, and encourage children to discuss their likes and dislikes. Ask them to suggest possible improvements to the prototype based on their thoughts and experiences(as Figure 1 shows). **Design Task:** Create a concept that teaches others about privacy or how to control it. Children start by sketching their design ideas on paper and then create design prototypes using DIY materials. **Showing Time:** Children present their designs and give each other feedback.
Design Session 4	Identify children's preferred methods for managing privacy.	**Design Task:** Design a way to teach or help others about privacy control. Children start by sketching their design ideas on paper. **Peer Reviews:** Children share their initial designs and provide feedback to others. **Presentation Design:** Children create their design prototypes using DIY materials like Lego, clay, and cardboard. They then refine their ideas and develop design posters to showcase their concepts and prototypes (as Figure 6 shows).
Design Session 5	Understand how children perceive privacy after the workshop and how parental involvement affects their privacy learning.	**Recap Time:** Review all activities from Design Sessions 1 to 4. **Presentation Time 1:** Children present their design posters, with each presentation lasting 10 minutes, followed by a 5-minute Q&A session. **Co-design with parent:** Children work with their parents to refine their designs. **Presentation Time 2:** Children and parents present their revised designs. Each pair has 10 minutes for the presentation, with a 5-minute Q&A session.

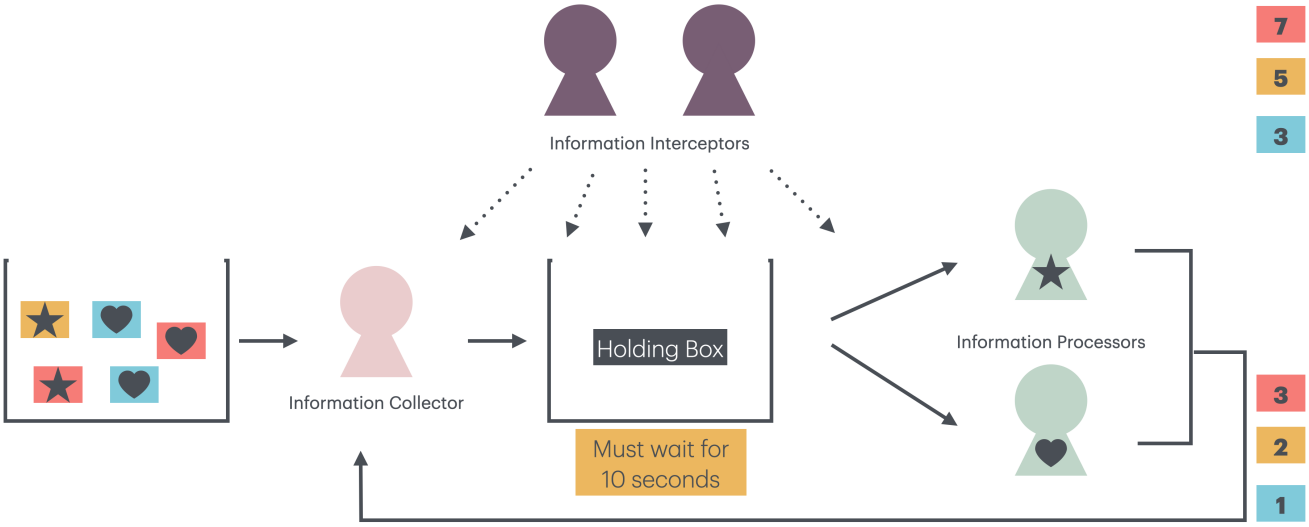

Figure 5: The Information Role-Played Game.

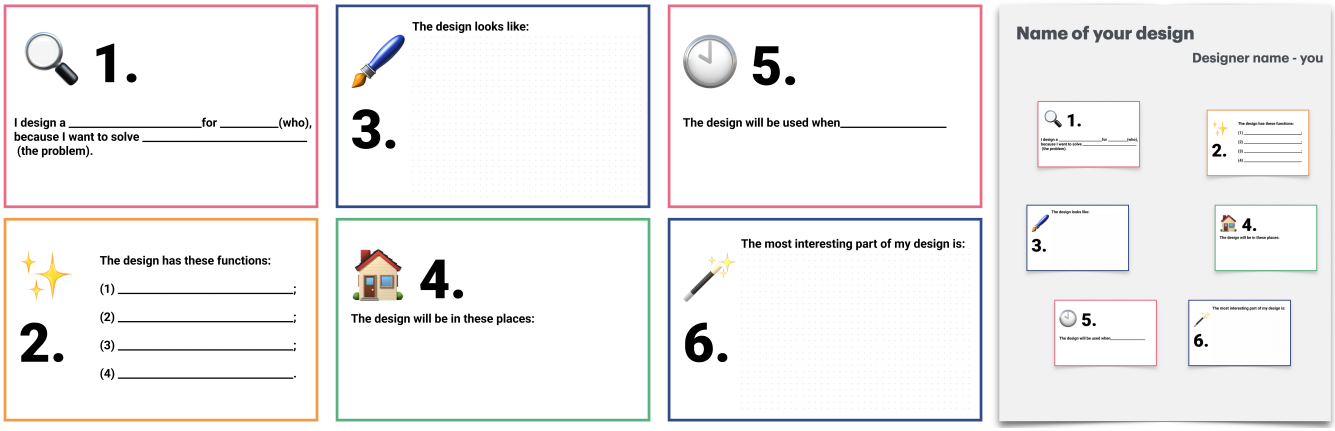

Figure 6: The Design Poster Template.