Co-Design Privacy Notice and Controls with Children

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

Xiaozheng Wang
Virginia Polytechnic Institute and State University
Blacksburg, Virginia, USA
xzwang@vt.edu

Shaddi Hasan
Computer Science
Virginia Tech
Blacksburg, Virginia, USA
shaddi@vt.edu

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

Abstract

Children, as digital natives, face increasing privacy risks and are required to make numerous privacy decisions daily. However, existing privacy notice and privacy controls mainly focus on adult users, remaining challenging for children, who may lack the literacy and developmental maturity to make informed decisions. To empower children to manage their privacy, it is essential to create accessible, comprehensible, and context-appropriate privacy notice and control designs. To fill the gap, we conducted a four-day co-design workshop with five children (ages 8-11). We uncovered children's critical challenges in current privacy notice and control, such as information overload, unclear terminology, and insufficient contextual or causal explanations. The findings reveal children's specific needs and expectations across key dimensions, including modality, timing, channel, and the types and functionality of privacy control. Based on these insights, we propose design implications to enhance children's ability to make informed privacy decisions and support their digital autonomy.

CCS Concepts

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

Keywords

Privacy Notice and Choice, Age-Appropriate Design, Design Workshops, Privacy Expectations

ACM Reference Format:
Lanjing Liu, Xiaozheng Wang, Shaddi Hasan, and Yaxing Yao. 2025. Co-Design Privacy Notice and Controls with Children. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3706599.3719886

CHI EA '25, Yokohama, Japan

ACM ISBN 979-8-4007-1395-8/25/04
https://doi.org/10.1145/3706599.3719886

1 Introduction

As children increasingly engage with digital technologies, they are exposed to various privacy risks, which they often struggle to navigate effectively. Prior studies highlight significant privacy concerns, including identity theft and cyberbullying, as well as frequent data sharing by children's apps with trackers and ad networks, despite protections like COPPA (Children's Online Privacy Protection Rule) [28, 35]. Although developers generally aim to protect young users, limitations in monetization options and unclear privacy guidelines often result in compromises on child data privacy [13]. Moreover, emerging technologies like wearables introduce new and complex privacy challenges [8, 26]. Privacy notice and controls, intended to inform users about data practices and allow them to make privacy decisions, are typically adult-centric, often failing to consider children's cognitive abilities and contexts [17]. Studies on privacy notice design have identified design spaces, including timing, modality, and privacy controls as critical to effective communication [15, 38]. Yet, the current privacy notices and controls remain challenging for children, who may lack the literacy and developmental maturity to make informed decisions. To empower children to manage their privacy, it is essential to create accessible, comprehensible, and context-appropriate privacy notice and controls designs. In this processing work, we present an initial exploration of the design principles for child-friendly privacy notice and controls design. Specifically, our research questions are:

- How do children interpret current privacy notice and privacy controls design?
- What design elements enable children to understand and act on privacy notice and privacy controls?

In the present work, we held co-design workshops with five children aged 8-11 to understand their needs for privacy notice and controls. The co-design workshop followed the privacy notice and controls design spaces [15, 38]. Through active participation, we aim to identify principles that inform the design of child-friendly privacy notice, empowering young users to make informed privacy decisions. In the discussion, rooted in our empirical evidence, we provided the design implications for child-friendly privacy notice and controls design principles. We propose that privacy interfaces can serve as valuable teachable moments for children to develop their privacy literacy, encompassing not only theoretical knowledge but also practical application in real-world contexts. These interfaces provide opportunities for children to actively engage

with privacy concepts, allowing them to translate abstract understanding into concrete decision-making skills that they can apply in their daily digital interactions. Then, we outlined the plans for future work, such as framing design implications, co-designing with children to come up with design prototypes, and evaluating design principles.

2 Related Work

2.1 Children's Unique Privacy Issues

Unsurprisingly, children are generally not aware of the privacy risks they may face, such as online tracking or game promotions [49], identity re-identification [31], except some basic privacy risks, such as information oversharing or revealing real identities online [48].

Privacy is a complex concept, and children's developing cognitive abilities and limited privacy skills often hinder informed decision-making. For example, many children did not talk about data loss as a risk, and they also failed to link personal data collection, potential misuse, and home IoT devices [42]. Third notes that children focus mainly on interpersonal privacy concerns, such as parental monitoring and threats from friends or hackers, while often overlooking commercial data risks [41]. Additionally, they tend to see mobile app data as static and localized, unaware of broader data collection and processing, which affects their ability to handle privacy challenges [40].

Children often use technology under parental supervision, sharing devices and personal information with family members, creating complex privacy dynamics. In home settings, robots that interact with multiple family members can expose private data to manufacturers and others [11, 16, 24]. Family locator apps, for example, collect both location and contact data, and some allow remote access to cameras or microphones [2, 23]. Parents also track children's activity and sleep through wearables, sometimes causing conflicts [18]. Many children do not realize that parents can access their audio recordings through smart toys, and older children worry about such privacy invasions [29].

Children's general knowledge of privacy often fails to prevent impulsive decisions, like downloading apps or sharing personal information online, as they lack the cognitive skills to apply privacy concepts to real-world choices [4]. This underscores the need for hands-on privacy support. However, current privacy designs seldom account for children's unique needs. Many family-oriented applications violate privacy regulations, posing long-term risks [35], and apps targeting children continue to share data with tracking apps despite COPPA regulations [3, 35]. Developers face challenges due to limited monetization options and unclear guidelines [14].

2.2 Privacy Notice and Privacy Controls Design

2.2.1 Privacy Notice. Informing users about privacy and data practices is crucial to enabling them to make privacy decisions. Privacy notices have shifted from being merely a legal compliance tool to one aimed at creating transparency for users. Privacy notices have become the de facto standard in informing users about how their personal data is collected, used, and shared by organizations [17]. These notices are typically provided to ensure transparency and compliance with privacy regulations, giving users insight into how their information is handled and what their rights are regarding data protection [17]. Florian Schaub et al. proposed a design space for privacy notice, including timing, channel, modality, and controls [38].

While privacy notices are widely studied and implemented for general users, there is a growing need to adapt them for specific audiences [30], particularly children [38]. Children are a vulnerable group, and their cognitive abilities, comprehension levels, and online behaviors differ significantly from those of adults. As discussed in Section 2.1, children often encounter unique privacy challenges and require immediate hands-on support when making privacy decisions or managing privacy practices. John Dempsey et al. proposed design guidelines for privacy warnings co-designed with children, aimed at intervening whenever children interact with or share personal data [10].

2.2.2 Privacy Controls. Providing users with effective privacy controls is crucial to empowering them to manage their data and protect their privacy. Privacy controls enable users to make decisions about what personal information they share, how it is used, and with whom it is shared [17]. The usability of privacy controls has been a significant focus of research. Feng et al. extended the established privacy notice design dimension [15] to improve the usability of privacy choices, including type, functionality, timing, and channel [38]. However, privacy controls design for children poses additional changes. Children's limited understanding of abstract privacy concepts, combined with their tendency to prioritize immediate gratification over long-term consequences, often leads to impulsive decision-making [4]. Research highlights that children struggle to navigate complex privacy settings, leading to unintentional oversharing or exposure to risks [48]. Child-centric privacy controls designs must account for these limitations.

2.3 Co-design 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 [12] - co-design has become a prevalent method in HCI and CCI research to understand children's needs and create 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 [12]. Co-design empowers children to propose solutions [37], facilitates a deeper understanding of their needs [44], and encourages reflection on the use of technology [9]. For instance, Wilson et al. used co-design to help verbal children express themselves through actions and interactions [44], while Wang et al. explored children's expectations for managing datafication through 10 co-design sessions [43]. Additionally, Woodward et al. examined children's conceptual models of intelligent user interfaces [45].

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 [22]. One example is "*The Watchers*," a hybrid computer and board game where children, acting as

secret agents, explore privacy-related scenarios [33]. Similarly, Kumar et al. examine how games and storytelling can shape resources for teaching children about online privacy [20].

3 Method

To investigate children's perceptions of online privacy notice and control, we held four co-design sessions.

3.1 Participants Recruitment

In this study, we recruited children between 8 and 11 years old for the following reasons: (1) By age 8, children begin to recognize the risks of sharing but generally display a trusting nature [27]. (2) Up to age 11, children still struggle with evaluating trustworthiness, identifying advertisements, and understanding privacy terms and conditions. While they value privacy, their comprehension of online privacy remains limited, and their reasoning often contains flaws [5, 31, 47]. (3) Compared to older teens (12–17 years old), children in this age group demonstrate lower competence in managing online privacy settings [7]. (4) Prior work has primarily focused on supporting privacy and security for children over age 12 [1, 32].

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 5 children for the initial workshop, who have some prior knowledge and experience with website and phone usage. Table 1 summarizes the participants' backgrounds and group allocation details.

3.2 Co-design Workshop

We held four weekly co-design sessions in October and December of 2024. Before the workshops, we introduced the study procedure to all parents and children and answered their questions. Then, we obtained the consent of all the children and the permission of the parents and conducted the demographic survey with parents. Each design session lasted around 1.5 hours with a self-contained topic and a set of activities. The outcomes from the previous sessions shaped the activities of the next sessions. This workshop was part of a long-term co-design activity with children, so the participants already had learned and discussed digital privacy and knew each other well before the workshop. We followed the framework of designing effective privacy notices and privacy choices [15, 38].

3.2.1 Design Session 1 (DS1): Interpretation of Current Design. The goal of DS1 was to familiarize children with privacy notice and controls while understanding their interpretations of current designs. We began the first design session by introducing common privacy notice and control designs and prompting children to discuss their understanding of these notifications and what they believed the messages conveyed. Next, we guided them through a *re-design* activity with printed versions of privacy notice and controls design. Each child first selected a design they found most interesting. To ensure accurate comprehension, all participants and the researchers engaged in a discussion about its meaning. Then, we asked the children to identify the "most terrible thing" in a design they disliked or found confusing and explain why it was problematic. Building on these critiques, the children re-designed the privacy notice or controls. Finally, each child presented their design ideas to the group, followed by a Q&A session to further illustrate their perspectives.

3.2.2 Design Session 2 (DS2): the Modality of Privacy Notice. The goal of DS2 was to explore children's expectations regarding the modality of privacy notice, including text, icons, images, sounds, and others. We began by discussing "How would you want to receive important privacy messages?", using common notice designs from both privacy contexts and everyday life, such as location data requests, traffic lights, and road signs. This discussion introduced children to different modalities and their effectiveness in conveying messages. Next, we presented children with common privacy scenarios, such as "An app wants to use your location," "A game needs your permission to access the camera," and "Who has access to the content you post?" Children then made choices about how they would prefer to receive these messages. Building on this discussion, each child selected a scenario they found most interesting and designed a "fun power" - a preferred modality (e.g., text, icons, images, or sounds) to effectively deliver the privacy message. Finally, they presented their design ideas to the group, followed by a Q&A session.

3.2.3 Design Session 3 (DS3): Type of Choice. In DS3, we aimed to explore children's expectations and needs regarding the types and functionality of privacy controls after they had become familiar with the modality. We began with interactive activities designed to help children understand different types and functions of controls by engaging with common control mechanisms in everyday life, such as light switches in a room, water faucets, and digital controls for adjusting brightness or volume on a computer. Following this hands-on exploration, we introduced children to common privacy control designs and facilitated a discussion about their interpretations. We asked them to reflect on the meaning behind each design, how they would make privacy choices using it, what potential consequences their choices might have, whether they liked or disliked the design, and why. Building on this discussion, we then invited children to design a new privacy control for their most-used or favorite app, specifying the types of privacy choices they would need to make and the control mechanisms they preferred.

3.2.4 Design Session 4 (DS4): Timing and Channel. In DS4, we explored children's needs and expectations regarding the timing and channels of privacy notices and controls. We began by introducing examples from everyday life to help children understand these concepts in familiar contexts. Following this, we engaged them in a *Finding Clues Game* [1] , where they experienced different timing and channel mechanisms firsthand. After the game, we presented various scenarios involving privacy notices and controls, such as

[1]The game follows a structured system where the researchers release different pieces of information at varying times and through different channels, requiring children to capture as much information as possible. Information is provided at six different timing points: (1) at setup, when children first enter the game area; (2) just in time, when they step into specific zones like the camera area; (3) contextually, when they perform certain actions; (4) periodically, with updates every three minutes; (5) persistently, where some information remains visible at all times; and (6) on-demand, when children request information from RAs. These messages are communicated through three channels: (1) primary, where the researchers speak directly to the children; (2) secondary, where RAs hand out written slips; and (3) public, where information is displayed on a TV screen.

ID	Age	Gender	Race/Ethnicity	Mother's Edu.	Father's Edu.	Devices Experience	Apps Experience	Attendance
C01	9	F	White	Bachelor	Graduate	Smartphone, Tablet, Laptop/PC, Smart TV, Gaming Console, Smart Speaker	YouTube, Roblox, Minecraft, Netflix, Hulu, Disney+	DS1-DS4
C02	11	M	White	Bachelor	Graduate			DS1-DS4
C03	9	F	White	Bachelor	Graduate			DS1-DS4
C04	10	M	Middle Eastern or North African	Graduate	< High School	Smartphone, Tablet, Smart TV, Gaming Console	YouTube, Facebook, Roblox, Discord, Minecraft	DS1, DS2
C05	8	F	Middle Eastern or North African	Graduate	< High School			DS1-DS4

Table 1: Participants' Demographic Information

location requests and data collection, and asked children to determine the most suitable timing and channels for delivering these notices. Through discussions, we further examined the reasoning behind their choices, gaining deeper insights into their preferences and decision-making processes.

3.3 Data Analysis

We recorded the video and audio for all workshops with the children's consent and their parents' permission. We also photographed all sketches and prototypes and took notes as needed, resulting in 325 minutes of video recording and 14 images. We also took field notes during the co-design sessions to document children's nonverbal body language, emotions, and other behavioral cues.

We first transcribed the videos using Kaltura[2], then manually reviewed and corrected the transcriptions. We followed previous research practices to analyze the session recordings [39, 46]. We captured both textual content and relevant visual data (e.g., a child pointed out a part of the design) and linked these details to the children's sketches and field notes. This was an iterative process until all researchers agreed on the links. We then conducted a thematic analysis on the transcriptions and notes [6]. 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 [36]. Two coders thoroughly reviewed all video transcripts and images multiple times and coded the data.

3.4 Ethical Consideration

As our research involved minors between the ages of 8 and 11, 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 Liu et al.'s work [25], we developed three strategies to help children protect their privacy: (1) We used child-friendly language to remind them not to share sensitive information. (2) When discussing sensitive topics, such as passwords and personal privacy, prior to the actual discussion, we explicitly instructed the children not to share specific details with us. (3) If a child showed any tendency or behavior toward leaking private information, the researchers immediately intervened to remind them not to share private information. We reported the incident to the parents after the session.

[2]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

4 Initial Results

4.1 General Understanding of Privacy Notice and Controls Design

Not surprisingly, children tended to ignore privacy notice and controls. Children dismissed repetitive or intrusive privacy notice, particularly during activities like gaming or app use. As one child explained, "*I just click OK so I can keep playing.*" They prioritized uninterrupted engagement over responding to unclear or redundant prompts, stating, "*It keeps asking me the same thing, and I ignore it.*"

Children associated control with a sense of empowerment, such as deciding who can access their data. One remarked, "*It's like being the boss of my account.*" However, some expressed distrust toward systems, with comments like, "*I don't trust apps knowing my location.*"

4.2 Challenges to Use Current Privacy Notice and Controls

4.2.1 Confusing Statements. Children struggle with abstract terms like "cookies," "permissions," and "data sharing." As one child remarked, "*Cookies are something you eat.*" Overly technical language in the privacy notice adds to the confusion, with comments like, "*I don't get what it's asking. It is confusing.*"

4.2.2 Lack of Context or Causality. Compared to adult users, children's limited life experience and digital knowledge make it difficult for them to comprehend the context and causality of privacy notices and controls. As a result, some children struggle to understand the rationale behind privacy notices, leading them to disregard or overlook their importance and preventing them from making informed privacy decisions. For example, they questioned the need for certain permissions: "Why does the calendar need my location? It's just for dates." Another noted, "Why does TikTok need my location? It doesn't make sense."

4.2.3 Overload of Information. Excessive text in privacy notice overwhelms children, leading to disinterest. Repeated prompts further desensitize them, reducing engagement. As one child explained, "*It will keep asking, so I just ignore it or choose 'Allow.'*"

4.3 Needs and Expectations of Privacy Notice and Controls

4.3.1 Modality. Children expressed a preference for straightforward notice that avoided excessive information or distracting elements. Visual cues, such as icons and illustrations, enhanced their understanding and engagement. They also expressed a preference for child-friendly visual expressions, such as cartoons and characters of a similar age to them. Additionally, they also preferred the simplified and polite text, exemplified by prompts like "*Would you like to allow TikTok access to your microphone?*" as it reinforced their sense of autonomy in using technology. Multi-modal auditory feedback, including sound and vibration, effectively captured their attention, with pop-up notice paired with sound cues (e.g., "*Ding-dong*") proving particularly engaging. Additionally, light indicators emerged as a favored modality due to their immediacy and clarity, offering a non-intrusive yet effective means of communication.

4.3.2 Timing. Children's engagement with privacy notice varies based on timing. At the set-up stage, they often overlook or skim notice without thorough attention. In-time notice, when presented clearly and accessibly, are effective but can sometimes feel confusing or overwhelming. Periodic notice must balance regular updates with avoiding excessive frequency, as too many can become irritating. Persistent notice that remain readily accessible are appreciated, though they risk causing frustration if overused. On-demand notice, while useful, may be ignored if it requires extra effort, as children favor ease of access.

4.3.3 Channel. Children found primary notice appealing due to their accessibility and ease of engagement, allowing for quick interaction without significant effort. In contrast, secondary privacy notice was often disliked, as they require additional steps to access, which can deter engagement. Public notice, however, was viewed favorably for their ability to foster social interactions and encourage peer engagement because children usually used the same apps with their friends, highlighting their heightened sensitivity to social influence and peer validation that differs from adults' typically more individualistic privacy decision-making.

4.3.4 Control Choice Types. Children demonstrated a clear understanding of binary and multiple-binary control options, such as "yes/no" toggles or buttons, which they found simple and intuitive. Their understanding of contextual controls, however, appeared less robust. For instance, when prompted with a notice about Uber accessing their camera, three girls chose "do not allow," reasoning that Uber drivers are strangers. This response highlights a gap in privacy literacy, as they struggled to grasp the nuanced contexts and causal relationships underlying such permissions. It is because children's tendency to apply concrete safety rules (don't share with strangers) rather than the situational risk assessment that adults more commonly employ.

4.3.5 General Expectations. Children expressed a preference for multiple notice approaches that were easily accessible and adaptable. They valued the ability to switch settings conveniently, stating, "*Because I can switch it anytime I want.*" The privacy notice needed to be clear and understandable, with language and visuals that provided both context and causality to support their decision-making. Children also emphasized the importance of real-time assistance when navigating privacy decisions. For example, when prompted to explain a preference for "*Keep only while using,*" one participant simply responded, "*I just feel like that,*" highlighting the need for guidance in articulating and reasoning through privacy choices.

5 Discussion and Future Work

5.1 Design Implication for Child-friendly Privacy Notice and Controls Design

The findings of this study underscore the need for privacy notifications and controls that align with the cognitive and emotional capabilities of children. Effective designs should prioritize clear, contextually relevant, and concise information, ensuring that children can easily comprehend the purpose and implications of their choices. For example, the interface design could implement a layered approach with essential information first (2-3 key points), include "Learn More" options that expand with age-appropriate explanations, and use progressive disclosure techniques with interactive elements, revealing additional details only when needed. Building on the children's preference for straightforward and actionable interactions, simple binary choices framed in accessible language can empower them to make informed decisions. And implementing tooltips that define complex terms in developmentally appropriate language could be useful To foster trust, transparent indicators and intuitive controls should be integrated, reinforcing a sense of autonomy and security. Multi-sensory notifications—such as engaging visual cues, sounds, or light indicators—can make privacy interactions more engaging and accessible. For example, we can provide a brief (5-10 second) cooling-off period for significant privacy decisions for children with immediate visual feedback confirming choices.

However, the timing and frequency of notifications must be carefully managed to avoid overwhelming children, as excessive or poorly timed prompts can lead to disengagement or dismissive behavior, as observed in the study results. These considerations provide a foundation for designing privacy interfaces that are both effective and child-friendly.

5.2 Privacy Interfaces as Developmental Tools for Children

While children and adults share common challenges with privacy notices and privacy choices, including confusion with technical terminology and frustration with repetitive notifications. And there are some efforts to show user privacy information effectively and interactively [19, 34]. However, our findings reveal considerations for children that require specialized design approaches rather than simply adapting adult interfaces. As mentioned in Section 4.2.2, children's heightened vulnerability stems from developmental factors and specific knowledge gaps in technological contexts that

standard privacy interfaces fail to address. Children also tend to ignore consequences and take risks.

Significantly, privacy interfaces represent valuable teachable moments beyond simple choice. Unlike other digital literacy, privacy is rooted in context and daily practice [21]. Rather than merely facilitating decisions, these interactions offer opportunities to develop privacy literacy through contextual learning. This perspective suggests a fundamental shift from viewing children's privacy interfaces as simplified versions of adult designs to seeing them as developmental tools that build competence through contextual learning. By embedding progressive privacy literacy elements within interfaces, designers can create experiences that support children in developing critical thinking skills about privacy while making informed decisions. This approach acknowledges children's agency while providing appropriate scaffolding for their evolving capabilities, addressing both immediate protection needs and long-term privacy competence development.

5.3 Limitation and Future Work

As a work in progress, we only have five children in our co-design workshop, in the future we will enhance diversity by incorporating more participants with different backgrounds. Regarding the further co-design workshop, we would include more privacy notice and controls material [19, 34] and get more insight from our participants. We will also adjust co-design protocols for varied ages to help them engage in interviews. Then, we also consider collaborating with more stakeholders, such as educators and personnel from privacy and design. This broader inclusion will provide richer insights into child-friendly privacy notice and controls design from different perspectives. Additionally, enhancing connections with user experience and user interface design in related literature and providing detailed data analysis will enhance future work.

Acknowledgments

We thank the anonymous reviewers for their valuable feedback and all the children and parents for their participation. We also thank Sasha Holt for the valuable support during the workshop. 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. doi:10.1145/3512904

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

[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. doi:10.56553/popets-2022-0108

[4] J. Craig Andrews, Kristen L. Walker, and Jeremy Kees. 2020. Children and Online Privacy Protection: Empowerment from Cognitive Defense Strategies. *Journal of Public Policy & Marketing* 39, 2 (April 2020), 205–219. doi:10.1177/0743915619883638 Publisher: SAGE Publications Inc.

[5] 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. doi:10.1145/3311927.3325324

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

[7] 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/

[8] 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.

[9] 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. doi:10.1145/3544548.3581134

[10] 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. doi:10.1016/j.ijcci.2021.100446

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

[12] 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. doi:10.1145/302979.303166

[13] 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. doi:10.1145/3411764.3445599

[14] 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. doi:10.1145/3411764.3445599

[15] 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. doi:10.1145/3411764.3445148

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

[17] Hana Habib, Yixin Zou, Yaxing Yao, Alessandro Acquisti, Lorrie Cranor, Joel Reidenberg, Norman Sadeh, and Florian Schaub. 2021. Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts. 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 63, 25 pages. doi:10.1145/3411764.3445387

[18] 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. doi:10.1145/3010915.3010936

[19] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (Mountain View, California, USA) *(SOUPS '09)*. Association for Computing Machinery, New York, NY, USA, Article 4, 12 pages. doi:10.1145/1572532.1572538

[20] 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. doi:10.1145/3202185.3202735

[21] 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. doi:10.1108/ILS-02-2022-0022

[22] 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. doi:10.1145/3585088.3589375

[23] Anastasia Kuzminykh and Edward Lank. 2019. How Much Is Too Much? Understanding the Information Needs of Parents of Young Children. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 3, 2 (June 2019), 52:1–52:21. doi:10.1145/3328923

[24] Min Kyung Lee, Karen P. Tang, Jodi Forlizzi, and Sara Kiesler. 2011. Understanding users' perception of privacy in human-robot interaction. In *Proceedings of the 6th international conference on Human-robot interaction (HRI '11)*. Association for Computing Machinery, New York, NY, USA, 181–182. doi:10.1145/1957656.1957721

[25] 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. doi:10.56553/popets-2024-0071

[26] 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. doi:10.1145/3613904.3642044

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

[28] Giovanna Mascheroni and Donell Holloway. 2019. *The quantified child: Discourses and practices of dataveillance in different life stages.* Routledge Handbook of Digital Literacies in Early Childhood, UK.

[29] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, Denver Colorado USA, 5197–5207. doi:10.1145/3025453.3025735

[30] Helen Nissenbaum. 2011. A contextual approach to privacy online. *Daedalus* 140, 4 (2011), 32–48.

[31] 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. doi:10.1145/3097286.3097338

[32] 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. doi:10.1145/3078072.3079722

[33] 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. doi:10.24908/ss.v12i3.4958

[34] Daniel Reinhardt, Johannes Borchard, and Jörn Hurtienne. 2021. Visual Interactive Privacy Policy: The Better Choice?. 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 66, 12 pages. doi:10.1145/3411764.3445465

[35] 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. PoPETs, Spain, 63–83. doi:10.1515/popets-2018-0021

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

[37] 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. doi:10.1145/3459990.3460725

[38] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. A design space for effective privacy notices. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security* (Ottawa, Canada) *(SOUPS '15)*. USENIX Association, USA, 1–17.

[39] 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. doi:10.1145/3628516.3655819

[40] 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. doi:10.1145/3411764.3445333

[41] Amanda Third, Delphine Bellerose, Juliano Diniz De Oliveira, Girish Lala, and Georgina Theakstone. 2017. *Young and Online: Children's Perspectives on Life in the Digital Age (The State of the World's Children 2017 Companion Report).* Technical Report. Western Sydney University.

[42] Sarah Turner, Nandita Pattnaik, Jason R.C. Nurse, and Shujun Li. 2022. "You Just Assume It Is In There, I Guess": Understanding UK Families' Application and Knowledge of Smart Home Cyber Security. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2, Article 269 (Nov. 2022), 34 pages. doi:10.1145/3555159

[43] 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. doi:10.1145/3544548.3580933

[44] 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. doi:10.1145/3290605.3300251

[45] 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. doi:10.1145/3173574.3174149

[46] 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. doi:10.1145/3585088.3589355

[47] 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. doi:10.1016/j.ijcci.2017.05.001

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

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