Understanding Research Related to Designing for Children's Privacy and Security: A Document Analysis

Priya C. Kumar*
College of Information Sciences and Technology, Pennsylvania State University
priya.kumar@psu.edu

Fiona O'Connell
University of Wisconsin, Madison
foconnell@wisc.edu

Lucy Li
University of Chicago
lucyyutingli@gmail.com

Virginia L. Byrne
Morgan State University
virginia.byrne@morgan.edu

Marshini Chetty
Department of Computer Science, University of Chicago
marshini@uchicago.edu

Tamara L. Clegg
College of Information Studies, University of Maryland, College Park
tclegg@umd.edu

Jessica Vitak
College of Information Studies, University of Maryland, College Park
jvitak@umd.edu

ABSTRACT

Many children are growing up in a "digital-by-default" world, where technologies mediate many of their interactions. There is emerging consensus that those who design technology must support children's privacy and security. However, privacy and security are complex concepts that are challenging to design for, and centering the interests of children is similarly difficult. Through a document analysis of 90 HCI publications, we examine what problems and solutions designing for children's privacy and security addresses and how this research engages with children. Applying Solove's privacy taxonomy, we find that research addresses a range of problems related to information collection, processing, dissemination, and invasion at the organizational, system, and individual levels. Children's participation in this research is largely limited to providing feedback rather than helping to guide the research itself. Based on these findings, we offer recommendations for designers to sharpen their privacy and security contributions and center children in their work.

CCS CONCEPTS

• **Social and professional topics** → User characteristics; Age; Children; • **Security and privacy** → Human and societal aspects of security and privacy; Social aspects of security and privacy.

*Corresponding Author

IDC '23, June 19–23, 2023, Chicago, IL, USA

ACM ISBN 979-8-4007-0131-3/23/06.
https://doi.org/10.1145/3585088.3589375

KEYWORDS

Children, Privacy, Security, Surveillance, Online safety, Design, Document analysis

ACM Reference Format:
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 *Interaction Design and Children (IDC '23), June 19–23, 2023, Chicago, IL, USA.* ACM, New York, NY, USA, 20 pages. https://doi.org/10.1145/3585088.3589375

1 INTRODUCTION

Many children are growing up in a "digital-by-default" world, where technologies mediate interpersonal, institutional, and commercial interactions [131]. In the U.S. and U.K., nearly all children go online at least once a day to view content, play games, and communicate with others [99, 114, 115]. Schools have been integrating computers, laptops, and online services into classrooms for decades [35, 100], and programs providing children their own devices were popular even before the COVID-19 pandemic drove many schools to operate virtually [124]. Brands harness influencer marketing to target advertising to children [21], even hiring young children who are already influencers [83, 150]. Many digital platforms that children interact with are owned by companies that profit from their users' data, creating a networked ecosystem driven by pervasive data tracking [9, 81, 87].

This encompassing "datafication" of children's lives poses significant threats to their privacy and security [24, 52, 58–60, 71, 80, 130, 132]. As a result, there is an emerging consensus that those who design technology need to consider its implications for children's privacy and security [80]. In particular, human-computer interaction (HCI) scholars have identified privacy and security as a key area for child-computer interaction (CCI) research [5, 50, 51] and advocate incorporating the needs of children into inclusive security and privacy research frameworks [145]. Policymakers are also

responding. Europe's General Data Protection Regulation (GDPR), which went into effect in 2018, includes specific provisions related to children [79]. Since then, lawmakers in the United Kingdom and California have enacted age-appropriate design codes requiring companies to incorporate privacy and security protections into the design of their systems [54, 146]. The U.S. Congress considered four child privacy bills in 2022 [11] (though none have passed as of April 2023), and policy analysts have mapped out how child data protection laws could be adopted globally [1].

Societies around the world are paying attention to the importance of designing for children's privacy and security, but privacy and security are complex, intertwined concepts [125, 127] that are challenging to design for [19, 26, 92, 151]. Philosophers and design scholars define design as an iterative process of defining problems and identifying solutions [25, 39, 122]. The field of HCI embraces user-centered design, or designing to meet the needs and desires of the people who use technologies, as a defining philosophy for iterating through these cycles of exploring and defining problems and solutions [123]. As such, CCI scholars strive to center children in their research and design processes, but putting these commitments into practice is difficult since working with children requires more in-depth ethical approval processes, specialized skills, and even a fundamentally different mindset toward research [48, 56, 62]. Thus, researchers involved in designing for children's privacy and security would benefit from a better understanding of the following questions:

- What problems does research related to designing for children's privacy and security address and how?
- How does research related to designing for children's privacy and security engage with children?

To answer these questions, we conducted a document analysis [14] of 90 publications related to designing for children's privacy and security spanning a decade of HCI scholarship. Our analysis differs from conventional meta-analyses of academic literature, which identify a phenomenon of focus and synthesize what research has found about it. Following Dourish and Anderson [26], we approach designing for children's privacy and security as a practice in which people engage rather than a discrete phenomenon to be defined. As such, our aim is to explore what designing for children's privacy and security does and how the process engages children. We focus on children ages 5-12 because children under 5 experience little autonomy over their bodies and activities [149] and prior work has considered how designers can support privacy and security for children over age 12 [3, 106]. Moreover, prior work has found that parents and teachers approach privacy and security as an adolescent issue [67, 68], suggesting an opportunity for designers to address the needs of younger children.

Drawing on privacy theorist Daniel Solove's taxonomy of privacy problems [127], we find that designing for children's privacy and security addresses a range of problems related to the collection, processing, and dissemination of information, as well as privacy invasion. Researchers in this design space address these problems through responses at three levels: organizational, system, and individual. Research projects primarily operate in the empirical, design, and technical paradigms, with none in the theoretical paradigm. Finally, while most projects do engage with children, their participation is largely limited to providing feedback rather than helping to guide the research itself. Based on our analysis, we recommend that designers whose work affects children's privacy and security use theoretical frameworks to identify and engage with privacy and security tensions, bring children further into the design process, and adopt an asset-based approach [153–155] to design that strengthens children's abilities to navigate privacy and security challenges.

The IDC community has a strong tradition of taking stock of existing scholarship and using it to inform the direction of the CCI field [56, 106, 138, 139, 157]. Our synthesis of HCI research related to designing for children's privacy and security complements such efforts and offers guidance to help researchers sharpen their privacy and security contributions and center children in their work.

2 BACKGROUND

To situate our analysis, in this section we discuss the importance of privacy and security for children, explain a theoretical framework of privacy and security problems, and review key considerations for engaging children in the design process.

2.1 Supporting Children's Privacy and Security

Dourish and Anderson argue that privacy and security do not exist as stable, unified concepts, but are "continual, ongoing accomplishments [that] are constantly being produced and reproduced" [26:328]. People experience privacy through the process of managing boundaries across different social spheres [103, 105], and contextual norms influence whether people regard particular flows of information as appropriate [10, 94]. In the early years of children's lives, parents and caregivers manage children's boundaries, and children acquire privacy expectations based on their experiences within the family setting [105]. As children develop cognitive skills related to information management, absorb social and cultural norms, form peer relationships, and expand their social spheres through school and other activities outside the home, their understandings of privacy also mature [149].

Privacy and security are important for children's development. Privacy helps children experience autonomy, which in turn supports several dimensions of psycho-social development, including identity formation, self-expression, independence, responsibility, resilience, prosocial behavior, trusting relationships, and critical thinking skills [95, 149]. In online interactions, privacy gives children the comfort to connect and communicate, engage in identity play, and push boundaries [78, 130]. At the same time, security measures are important to protect children from "undesirable" experiences and protect systems from viruses, malware, and other threats that children might unintentionally encounter [37]. The use of digital technologies can threaten several dimensions of children's privacy. Technologies can monitor children's physical whereabouts, document their communication with others, track their personal information, and influence their decision making [97]. As a result, policymakers have called on the technology industry to better support children's privacy and security in the systems they create [54, 146].

HCI scholars, especially those in the IDC community, are at the forefront of designing for children's privacy and security. Recent work has explored how children conceptualize digital privacy and security issues [13, 27, 68, 136, 144, 164, 166] and examined how parents [68, 136, 164], teachers [67, 84], and app developers [29] approach digital privacy and security concerns. Research teams have created tools to help children learn about privacy and security issues, including an IoT storytelling program [7], interactive comics [135, 162], mobile apps [16, 165], online games [16, 41, 69, 85, 101] and social media simulators [23, 167]. More broadly, researchers have analyzed existing educational materials and synthesized recommendations and opportunities for future work [107, 108, 163]. Our analysis complements this work by specifying how design addresses the privacy and security problems children face through digital interactions.

2.2 Identifying Privacy and Security Problems

To better understand the myriad privacy and security problems facing children, we draw on legal scholar Daniel Solove's taxonomy of privacy problems [127]. Solove acknowledges that privacy "is a concept in disarray" [127:1], but his goal is not to pinpoint a core definition of privacy. Rather, he embraces the plurality of meanings that privacy encompasses and instead focuses on the kinds of activities that can raise privacy concerns, especially when considering new technologies. His taxonomy contains sixteen privacy problems organized into four categories: information collection, information processing, information dissemination, and invasion.

Information collection activities include surveillance and interrogation, which involve gathering information in ways that can become problematic. Information processing activities affect how information "is stored, manipulated, and used" [127:104]. These include aggregating various pieces of information about someone, linking information with someone's identity, storing information insecurely, using information for different purposes than what someone agrees to, and preventing people from accessing or modifying their information. Information dissemination activities concern what happens when information circulates. These include breaching confidentiality, disclosing information in a way that can harm one's reputation, exposing one's body or grief, making information about someone more easily accessible, threatening to disclose information via blackmail, appropriating one's identity without their consent, or spreading distorted or otherwise misleading information about someone. Finally, invasion activities occur when someone intrudes on another person's physical, psychological, or digital space or when someone interferes in another person's decision making.

Though Solove devised the taxonomy to support law and policy development, it can also be useful for researchers and designers. Many designers recognize that privacy is important to protect but struggle to integrate privacy into the systems they build [151]. Solove's taxonomy discusses privacy in terms of specific problems rather than abstract concepts, like secrecy. By framing privacy as a set of problems, the taxonomy turns privacy into something concrete for designers to solve. Design is about creating solutions that "work" not only in a technical sense but also socially, culturally, aesthetically, and ethically [39]. Thus, Solove's taxonomy can make privacy more legible to designers by framing it as a problem they can address through design. At the same time, the taxonomy's focus on use of information is also broad enough that it can be applied to the various domains in which researchers and designers work. In this paper, we identify which problems, as defined by Solove's taxonomy, research related to designing for children's privacy and security addresses.

2.3 Designing For and With Children

A core value in the CCI community is that children should be involved in the design process [56, 157]. Druin [28] identifies four roles a child can play in this process: user, tester, informant, and design partner. These roles invite participation from children in different ways. For example, children's input can be indirect (e.g., when adults solely observe children) or more direct (e.g., when adults seek written or verbal feedback from children about their experiences or perspectives). Deeper forms of engagement with children include dialogue, where children share their own ideas with adults, and elaboration, where children iterate on ideas generated by others to create something new. Others have extended this framework to more fully characterize child-adult relations in design and research [160] as well as to articulate how children lead participatory design processes [55, 121] and take on new roles within it [61]. Using participatory methods does bring children into the design process, but truly centering children's interests also requires considering what theories underpin a project as well as how the outcomes of the process affect children [48, 62]. Researchers and designers must therefore be intentional and reflective about how they work with children.

HCI scholars note that design must account for the ways stakeholders and external factors (e.g., market forces, regulations) influence technology adoption [17, 34]. Those designing technologies for children are well positioned to take a more holistic, stakeholder-centered approach to design, given the recognition that parents, teachers, caregivers, and peers influence how children use technology [49, 111]. However, designers should avoid prioritizing stakeholder interests over children's needs and desires. For example, many technologies intended to support children with autism focus on changing children's behaviors to match the expectations of a primarily neurotypical society [128]. This positions children's perspectives and experiences as secondary and prioritizes the desires of neurotypical people. Spiel et al. advocate that designers treat autistic children as partners in the design process, working with "autistic children as stakeholders much earlier, when it concerns the definition of needs and desires a technology should address" [128:22]. This embodies the disability rights movement's credo of "nothing about us without us," which calls on designers to heed people's own definitions of problems and solutions, especially when working with people who experience marginalization [129].

With regard to designing for children's privacy and security, "nothing about us without us" pushes researchers and designers to prioritize children's own understandings of and responses to privacy and security issues, rather than treat children's views as underdeveloped or naive. In this paper, we consider how and to what extent research projects involving designing for children's privacy and security engage with children in their work.

Table 1: Search Queries and Results

Source	Search Query[a]	Results	Included
ACM Digital Library	child* AND design AND (priva* OR secur* OR safe*) in publication title, abstract or keywords	277	56
IEEE Digital Library	child* AND design AND (priva* OR secur* OR safe*) in all metadata	268	22
USENIX Proceedings	children	7	3
International Journal of Child-Computer Interaction	privacy OR private OR security OR secure OR safe OR safety in Title, abstract or author-specified keywords	6	4
Proceedings on Privacy Enhancing Technologies (searched through Sciendo)	child* AND design AND (priva* OR secur* OR safe*)	5	2
International Journal of Human-Computer Studies	child AND design AND (privacy OR private OR security OR secure OR safe OR safety) in Title, abstract or author-specified keywords	2	2
Behaviour & Information Technology (Searched through Academic Search Ultimate)	child AND design AND (priva* OR secur* OR safe*) in abstract	2	1
International Journal of Human-Computer Interaction (Searched through Academic Search Ultimate)	child AND design AND (priva* OR secur* OR safe*) in abstract	0	0
TOTAL		567	90

[a] The use of an asterisk (*) in search terms includes variations of the root word. For instance, priva* would yield results that mention the terms "privacy" and "private." Some sources did not permit the use of asterisks in searches.

3 METHODS

In this section, we explain how we assembled and analyzed our corpus of HCI publications related to designing for children's privacy and security.

3.1 Assembling Our Corpus of HCI Research

We first consulted with university reference librarians to develop a search strategy for assembling a corpus of HCI publications related to designing for children's privacy and security. We identified the digital libraries of the ACM, IEEE, and USENIX as relevant sources. We then used Google Scholar to identify top HCI publication venues and added three sources that were not indexed in those databases: *International Journal of Human-Computer Studies*; *Behaviour & Information Technology*; and *International Journal of Human-Computer Interaction*. We also added two sources specific to child-computer interaction (*International Journal of Child-Computer Interaction*) and privacy and security (*Proceedings on Privacy-Enhancing Technologies*).

In January 2020, we searched each source using a combination of terms related to children, design, privacy, security, and safety (see Table 1). We included the term "safety" because privacy and security work related to children often occurs under the aegis of online or cyber safety [77, 130, 148]. To manage the scope of our analysis, we restricted our search to publications from the preceding decade (2009-2019). The searches yielded 567 results. Table 1 lists the sources, keywords, and number of results per source, in descending order.

The lead author examined each abstract, consulting the full text when necessary to understand the publication. Based on this, she developed a list of exclusion criteria and discussed it with the co-authors. Once the team finalized the criteria, the lead author re-examined all results and identified which publications to include. A second author reviewed each decision, and the authors discussed discrepancies until reaching consensus. In two cases, two publications discussed the same project, so we included the one that contained the most detail. We excluded 477 results for the following reasons:

- They were not in English.
- They did not report a research or design contribution (e.g., the publication was a workshop proposal or keynote address abstract).
- They focused only on children under age 5 or over age 12.[1]
- They focused on non-computing technologies (e.g., designing a secure car seat).

The final corpus contains 90 publications, encompassing journal articles, conference proceedings, posters, late-breaking work, works-in-progress, and workshop papers. (See the A Appendix for a full list.)

3.2 Analyzing Our Corpus

Our analysis followed the three stages of document analysis: (1) gaining familiarity with the data, (2) examining the data in-depth, and (3) interpreting the data based on the study's driving questions [14]. The familiarization stage occurred as we reviewed the search results and assembled the corpus. In the examination stage, we employed structural coding to identify the portions of each publication

[1]While our focus is research involving children ages 5-12, we included publications that encompassed but went beyond this range (e.g., ages 7-15).

relevant for our analysis [118]. Two authors coded each publication for its motivation, research questions, theories used, definitions of privacy and security, methods, findings, and contribution. In the interpretation stage, we conducted four rounds of pattern coding, which integrated data from the structural coding into categories relevant to our research questions [118].

The first two rounds of pattern coding focused on problems and solutions. Here, the unit of analysis was a complete thought (i.e., a sentence to a paragraph of text from a publication). Publications varied in (a) the degree to which they engaged with privacy and security issues and (b) the way they engaged the topics. Some publications focused entirely on privacy and security issues, while others only discussed them briefly. Additionally, some publications mentioned privacy problems but did not discuss solutions and vice versa, while others mentioned several privacy issues but only focused on a few. Given that all publications did not engage with privacy and security equally, attempts to draw quantitative comparisons across publications (e.g., X percent of publications address Y privacy problem) would not accurately represent the corpus. The problem round of coding used Solove's sixteen privacy problems as codes [127]. The solutions round used three inductively generated categories as codes: organizational responses (e.g., steps that those who design technologies or use children's data, including companies, developers, or agencies, can take), system responses (e.g., components, elements, or features in the technologies themselves that address privacy and/or security issues), and individual responses (e.g., steps that children and/or the adults around them, such as parents or teachers, who use technologies can take).

The third and fourth rounds of pattern coding focused on research paradigms and engagement with children. Here, the unit of analysis was the publication, since each element could be assessed for every publication (i.e., all publications operated within a paradigm and all publications either did or did not engage with children), making quantitative comparisons possible. The paradigm round used the six categories by which CSCW organizes paper submissions as codes: empirical-qualitative, empirical-quantitative, empirical-mixed methods, design, technical/systems, and theoretical. The child engagement round used Druin's four types of child engagement [28] as codes: indirect, feedback, dialogue, elaboration, plus an additional "no involvement" code when the publication did not report any engagement with children. At each stage, the authors discussed the coding and resolved any differences by consensus.

3.2.1 Limitations. We acknowledge three limitations of our research approach. First, by focusing on publications that mentioned keywords related to privacy, security, or safety, we may have overlooked work that has privacy and/or security implications (e.g., involves collecting sensitive data from children) but where researchers did not state this explicitly. Second, by limiting our search to terms in publication titles, keywords, and abstracts, we may have inadvertently excluded some potentially relevant results. Third, since our search was conducted in 2020, this analysis does not include the most recent publications on designing for children's privacy and security. Nevertheless, we believe that the breadth of work in our corpus, spanning a decade of scholarship, offers a foundation for understanding the contributions of designing for children's privacy and security. Indeed, the absence of post-2020 publications in our corpus presents a unique opportunity for future work to compare our analysis with recent scholarship to identify whether and how the global COVID-19 pandemic affected research on designing for children's privacy and security.

4 FINDINGS

In this section, we present our findings in response to the research questions that guided this study. The first three findings address our first research question, about what problems designing for children's privacy and security address and how. The fourth finding addresses how research in this design space engages with children. As explained in Section 3.2, we only present quantitative results for findings three and four, where the unit of analysis was the publication.

4.1 Finding 1: Designing for Children's Privacy and Security Addresses Problems Related to Information Collection, Processing, Dissemination, and Invasion

Our analysis found that research related to designing for children's privacy and security addresses problems across all four categories in Solove's taxonomy. We detail each below.

4.1.1 Information Collection. Information collection concerns involve the problem of surveillance, which Solove defines as "the watching, listening to, or recording of an individual's activities" [127:104]. Research in our corpus addresses issues such as parents monitoring children's digital interactions [40, 116, 166] or using technologies to track children's location [30, 31, 33, 140] out of a desire to protect children from threats. At the same time, research notes that parents can also find such measures ineffective [44], unnecessary [140], or invasive [70]. It recognizes that children may feel comfortable with some form of parental monitoring [89] but resist monitoring that is constant [8] or imposed on them with little explanation [40]. Conversely, it acknowledges that children may also use IoT devices to surveil parents, siblings, or peers, with little recognition of the potential negative consequences [64].

4.1.2 Information Processing. Information processing concerns largely focus on insecurity, which encompasses "glitches, security lapses, abuses, and illicit uses of personal information" [127:127]. More specifically, the field of information security aims to prevent problems related to breaches of confidentiality, loss of data integrity, and unauthorized access to information [119]. Research in our corpus focused on how children may fall victim to phishing or malware attacks [44, 72] and how they struggle to use security features such as passwords [53, 110, 112, 164], which can leave systems vulnerable to unauthorized access. Researchers recognize that systems themselves may also be vulnerable to attack. McReynolds et al.[90] note a hack of one smart toy company that exposed the data of more than 200,000 children, including photos and chat messages. Since IoT devices such as smart toys often transmit data to cloud storage as part of their regular operations, malicious actors can hijack such channels and gain remote access to components such as cameras or microphones. Beyond putting children's data at risk, researchers acknowledge that such attacks could put a child's

physical wellbeing and safety at risk if the actor uses the device to communicate with a child or locate them [30, 31, 64, 133].

Aggregation, or the gathering of many pieces of information about someone, is also a concern [127]. Research in our corpus notes that digital platforms accumulate data from children who provide it, for instance when submitting a search engine query or filling out an online form, and from cookies or other trackers [137]. Apps and IoT devices bring together various forms of data, including contact information, location information, messages, photos, videos and more gathered through various channels and sensors [76, 133] and accumulated over time [64]. Parents and children alike may not recognize or discuss the concerns related to such tracking [126, 166]. Beyond systems, government agencies may also compile data about children and families receiving social services [15, 46].

Aggregation, whether by systems or agencies, means that entities have large amounts of personal data at their disposal. Two related problems are identification and secondary use. Identification involves connecting information to a specific person [127]. Research in our corpus acknowledges that children may feel self-conscious sharing certain kinds of information, for instance, about their fitness [38], or they may become vulnerable to insults or humiliation if information they share online is linked to their identity [82]. Secondary use arises when entities use information for purposes other than what an individual agrees to. Beyond user agreements, regulations may also constrain how entities can use information. For instance, the U.S. Children's Online Privacy Protection Act (COPPA) limits how entities can use children's data. Research notes that several software development kits forbid app creators from using them in apps for children, yet many children's apps use them anyway, in some cases for targeting advertising [113].

The problem of exclusion arises when people do not know what information an entity has about them and cannot access or change that information [127]. Research in our corpus notes that children seek transparency; for instance, they may find it disconcerting or "creepy if a technology [does] not intentionally give enough information for them to fully understand it" [159:7]. Research recognizes that even when technologies do explain their practices, parents are usually the ones providing consent, often without fully reviewing or understanding a company's data management practices [90]. Children and parents alike may not realize what information a device collects or distributes [64, 90, 133].

4.1.3 Information Dissemination. Information dissemination concerns center on disclosure, which involves divulging information that is true or accurate but also potentially sensitive [127]. Research in our corpus observes that from a young age, children recognize that certain kinds of information are more sensitive than others, but that they may struggle to discern when it is and is not appropriate to disclose such information [164, 166]. Children may be quick to disclose information when they are experiencing challenging emotions, such as loneliness, or when they believe doing so can make a positive contribution to a situation, even if such disclosure could result in negative consequences [64]. For instance, research finds that children may use social media or IoT tools to chat with people they don't know, or they may eagerly fill out online forms or provide information in mobile games if they believe they will gain something in return [64, 137, 166].

Research in our corpus recognizes that parents also experience tensions when it comes to disclosing information about their children. For instance, posting about their children on social media can help parents gain social support and express their identities, but children themselves may not welcome such disclosure about them [4, 91]. Parents whose children experience challenges such as health problems can feel stuck between wanting to protect their child's privacy and needing to disclose information to health providers and school officials [143]. Teachers may also struggle with disclosure decisions, as classroom technologies often request (or require) information such as children's names, email addresses, or birthdates [67]. Furthermore, the emergence of conversational technologies like robots that personalize their interactions to users raises questions about how children may react if a technology seemingly "learns" something private about them [73]. And the networked nature of the digital ecosystem means that children's apps may (inadvertently or not) disclose location data or contact information such as email addresses and phone numbers [113].

Another concern related to information dissemination is increased accessibility, which arises when information that has already been disclosed in some way is available to a wider audience than one may have initially realized [127]. As digital interactions often create some kind of record, increased accessibility is the default condition of many aspects of people's lives, especially for children. For instance, research in our corpus notes that where parents used to store photographs of their children in albums or shoeboxes, many now post them on social media, making them visible to others [91].

4.1.4 Invasion. Invasion concerns pertain to intrusion, or "incursions into one's life, [which] disturbs the victim's daily activities, alters her routines, destroys her solitude, and often makes her feel uncomfortable or uneasy" [127:162]. Research in our corpus acknowledges that parents may intrude on children by going through their phones, reading their messages, or listening to recordings they make on smart toys [90, 98, 116]. Children may also get frustrated when siblings, peers, or parents bother them while they're doing something online [152, 164]. Children with divorced parents may also find it hard to find an uninterrupted time or space to connect with each of their parents alone [156].

In sum, research in our corpus addresses a range of privacy problems that span all four categories of Solove's taxonomy [127]. The next section explains how research in our corpus addresses these concerns.

4.2 Finding 2: Designing for Children's Privacy and Security Responds to Problems at Organizational, System, and Individual Levels

Through our analysis, we discerned three levels at which research on designing for children's privacy and security offers responses: organizational, system, and individual.

4.2.1 Organizational Level. The organizational level includes companies, government agencies, or individual developers that create technologies for children as well as use children's data. We found that researchers advocate that if children are potential users of a technology or service, organizations should consider their interests

in the design process [90]. Scholars have developed frameworks with guiding questions and activities that developers can use to identify how their technologies might affect children [64, 159]. Research on designing for children's privacy and security advocates that organizations follow relevant regulations, develop data practices that align with user norms, and explain those practices in a clear manner so users meaningfully understand them. For instance, COPPA restricts websites and online service operators from knowingly collecting data from users under age 13 unless they fulfill certain requirements, such as acquiring parental consent [32], and one study found COPPA's provisions align with parent expectations regarding children's data management [6]. Several research teams have designed systems to detect potential violations of COPPA among mobile apps [12, 76, 113], and one created a tool that developers can use to explain how they comply with the law [74].

4.2.2 System Level. The system level focuses on the technologies themselves and how they manage children's data and structure the interaction experience. We found that researchers recognize that design decisions directly affect whether users experience privacy problems, and they take several steps to mitigate or prevent such problems in technology system design. For instance, systems can avoid collecting personal information from children [38], or they can collect information through minimally invasive means. In another example, systems can use sensor data to infer people's presence rather than image data, which can be more identifying [93, 109, 161], or transmit photos rather than video [143]. Systems can document user interactions with an ID number or pseudonym rather than a child's name [30, 38]. To address security concerns, systems can encrypt data that must be stored or transmitted, restrict system access to authorized users, and require users to authenticate before gaining access, usually through a password. Noting that password management can be challenging for children, one research team created a system through which parents could authenticate access on their children's behalf [53].

Researchers also recommend design decisions that incorporate privacy into the user experience for children. Systems that involve communication can create distinct spaces for group (or public) interactions and one-to-one (private) conversations [75, 152, 156]. They can also include indicators that show when a user is available for interaction [142, 143]. Systems related to learning can include spaces where children can work individually before sharing their work or discussing it with others [57, 96]. Systems that involve recording can include indicator features to make users aware when such recording occurs [33, 47, 90, 159]. Finally, systems can also incorporate features to help children navigate challenging situations online, such as features that identify risks, offer advice or suggestions to children, and help children initiate conversations with parents [8, 89].

4.2.3 Individual Level. The individual level includes children who interact with digital technologies, as well as adults who may create or manage children's data. As part of their cognitive and social development, children learn how to use technologies and manage information flows. Since they absorb a great deal of this know-how at home, researchers encourage children and parents to discuss these topics and help children navigate questions, for instance, related to what is appropriate to post online or how to determine when technology is trustworthy [91, 159, 166]. Researchers also note a variety of actions that children and parents can take to address privacy problems. For instance, using a pseudonym can mitigate identification [4, 67, 82, 166]; covering laptop cameras can avoid surveillance [159]; and seeking out private spaces or channels to engage with others can minimize intrusion [152, 156]. Researchers note that educational efforts can help children and adults better understand technology-related privacy and security problems and how to address them. Several teams offered recommendations to inform the creation of educational materials for children [13, 45, 67, 69], while others designed and tested materials such as an interactive comic book [162], a digital game [86], and a phishing lesson [72]. Acknowledging that adults would also benefit from education, one team held a public workshop for educators focused on mitigating threats from smart toys [133].

In sum, researchers offer a variety of strategies designers can use to address children's privacy and security problems at the organizational, system, and individual levels. We now explain the kinds of contributions research on designing for children's privacy and security make.

4.3 Finding 3: Research Projects Operate in Empirical, Design, and Technical Paradigms, But Not in the Theoretical Paradigm

Our analysis also considered the paradigms through which research projects related to designing for children's privacy and security approach their work (See Figure 1). Our corpus contained no publications from a theoretical paradigm, which left three categories of methodological orientation: empirical (including qualitative, quantitative, and mixed methods), design, and technical. Forty percent of the publications in our corpus (36/90) worked in the empirical paradigm. These publications employed conventional social science research methods, including interviews [e.g., 90,164], focus groups [e.g., 67,166], surveys [e.g., 6,91], and the analysis of materials such as news articles or drawings [e.g., 44,98], often with the goal of informing the design of technologies related to children's privacy and/or security. A few studies reported results of experiments that measured the effectiveness of educational materials or the consequences of a design feature [e.g., 72,73]. User studies or field tests in which researchers deployed a system and evaluated it [e.g., 33,38] were included in the empirical category, since their contribution focused less on the design of the system and more on the way it was used.

About one-third of the publications in our corpus (31/90) worked in the design paradigm. They used design methods such as user-centered or participatory design to inform the design of technologies or to create prototypes of games, apps, or password mechanisms [e.g., 8,53,69,86,89,159]. Finally, a quarter of the publications in our corpus (23/90) worked in the technical paradigm. They proposed, prototyped, or built systems, often for tracking children, monitoring or controlling children's online activities, or detecting data flows in children's apps [e.g., 113,137,158]. Our analysis demonstrates that research related to designing for children's privacy and security operates from diverse perspectives but has yet to consider how theory intersects with this design space.

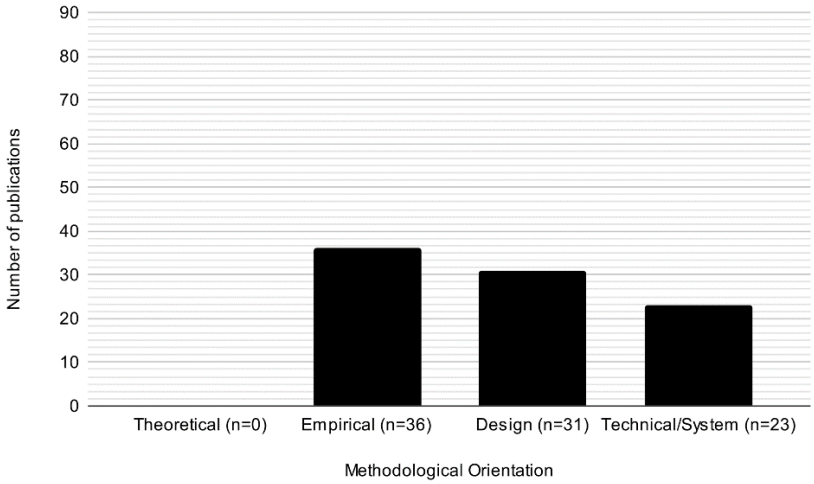

Figure 1: Methodological Orientations of Research Related to Designing for Children's Privacy and Security

4.4 Finding 4: Research Projects Largely Engage with Children, But Primarily by Gathering Their Feedback Rather Than Involving them in the Design Process

Finally, our analysis explored how research projects related to designing for children's privacy and security engage with children (See Figure 2). Less than half of the publications in our corpus (37/90) reported no engagement with children. Some publications scoped their research questions to focus on adult perspectives regarding technologies that affect children, such as parents' opinions on child tracking and monitoring technologies [70, 140], parents' expectations related to data collection and internet-connected toys [6], and educators' experiences managing children's privacy and security in classroom technologies [67]. Others presented solutions intended for adult stakeholders, such as tools to help app developers and regulators check for COPPA compliance [74, 76, 113]. In several publications, a system design constituted the intellectual contribution, including a software architecture for content filtering [137], a child location-tracking system [22], and a child-friendly social networking system [2]. These publications presented the systems as offering a social benefit, primarily protecting children, but the work largely attended to technical issues such as system functionality.

Conversely, more than half of the publications in our corpus (53/90) reported engaging with children in the design process, meaning researchers collected data from children using methods like observation, interviews, experiments, and participatory design. Eight publications involved children *indirectly*. Researchers collected and analyzed existing materials from children, such as online app reviews children had written [40]; examined aspects of children's interactions with technologies, such as the kinds of passwords children create [18]; or tested systems with child users without seeking any direct feedback from those children [158]. Thirty-three publications sought *feedback* from children. Researchers interviewed children about how they experienced or conceptualized privacy and security [15, 90], sought children's input on prototypes that researchers created [53, 86], or field-tested systems with children and inquired about children's experiences [38, 143]. Four publications involved children in *dialogue*, which encompassed workshops where children developed ideas for new Internet of Things technologies [64] or online safety educational materials [45]. Eight publications involved children in *elaboration*; researchers conducted cooperative inquiry with teams of child and adult research partners to design new technologies [89, 159].

When researchers reported engaging with children, feedback relations were most common, with far fewer instances of dialogue and elaboration. This is understandable given that conducting design work with children typically requires more resources and time than interactions such as observing or interviewing children. In sum, our analysis indicates that most research projects related to designing for children's privacy and security are incorporating children's perspectives into their work, though they primarily approach children as sources of information rather than collaborators in research.

5 DISCUSSION

Our analysis found that the published literature on designing for children's privacy and security addresses a variety of privacy problems spanning all four categories in Solove's taxonomy [127], responding to such problems at the organizational, system, and individual levels. We also identified opportunities for this work to explore intersections with theory and engage with children more deeply in the design process. We recognize that implementing these recommendations into designing for children's privacy and security is challenging. Thus, based on our analysis, we developed a set of guiding questions that researchers can use as a starting point (See Table 2). These guiding questions pertain to each stage of the design process and build on both of our research questions. The first set of

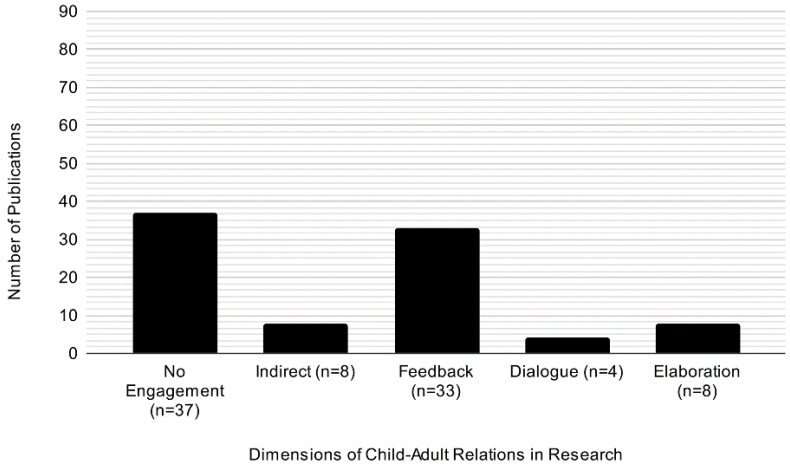

Figure 2: Children's Engagement in Research Related to Designing for Children's Privacy and Security

Table 2: Questions to Ask Throughout the Design Process

	Starting a Project	Defining the Problem	Developing Solutions	Reflecting Before Launch/Iteration
Privacy and Security Issues	Why is privacy and security important for this project? How might children's privacy and security apply to this project?	Which privacy and security problems apply to this project and how do they connect? What additional privacy and security needs or constraints exist in the environment children are situated in for this project?	At what level (organizational, system, individual) can this project address the issue? Do the features in our designs pose any additional privacy and/or security problems for children?	Have we addressed the privacy and/or security problem(s)? How can our solution be taken up at other levels (organizational, system, individual)?
Engagement with Children	How can we engage children in the design process?	What skills and capabilities do children have that could help them with their privacy and security related to our project?	How can we build on children's skills and capabilities with respect to privacy and security in our project?	In what ways has our work strengthened children?

questions can help researchers pinpoint how their work affects children's privacy and security, while the second set of questions can help researchers discern how their work can engage with children.

Since the publications in our corpus cover a variety of research topics and methods, these guiding questions are intentionally general. However, we believe many kinds of researchers, from those in the IDC community who already conduct participatory design with children to computer scientists who design algorithms to flag content that is inappropriate for children, would benefit from considering these guiding questions. Recent work has highlighted the need for those who develop and design technologies to engage with the ethical and social implications of their work [20, 42, 102], and we believe that this includes those whose work affects children's privacy and security. We encourage future work to examine how these guiding questions may translate to different domains of design that can affect children's privacy and security.

Based on our analysis, we offer three recommendations for researchers whose design work is related to children's privacy and security. First, we encourage researchers to use privacy and security theories and frameworks to identify and engage with tensions in the design process. Second, we suggest ways that researchers can engage children in their design work. Finally, we advocate that

researchers go beyond a user-centered design approach toward an asset-based approach that strengthens children's abilities to navigate privacy and security challenges.

5.1 Use Privacy and Security Theories and Frameworks to Work Through Tensions in Design

The guiding questions in Table 2 ask researchers to pinpoint what privacy and security issues are relevant for their work and to consider how they can address the issues. Privacy and security are complex concepts with a variety of meanings [125, 127], which means that projects will likely touch on several privacy and security issues, some of which may seem at odds with one another. Drawing on existing theories and frameworks can help researchers navigate these tensions. Since design is an iterative process of creating solutions to address problems [25, 39, 122], researchers may find Solove's taxonomy [127] an approachable framework to use in their work, given the taxonomy's explicit focus on problems.

For instance, the problem that Solove calls insecurity, or the concern that children's digital interactions can put themselves or their data at risk, is significant. One common response that appears in our corpus is to design parental controls or monitoring systems [36, 104, 120]. It is important for such systems to themselves be secure, and one research team explained several measures they took in this vein: local data storage, "encryption options, requirements for strong user passwords, methods to ensure child users do not turn off the software, and various software and data integrity checks [104:35-36]. However, parental control and monitoring systems also raise privacy questions related to the problems Solove labels surveillance and invasion [40], something these researchers did not discuss in their paper [104]. Indeed, other researchers suggested the parental control systems they designed helped protect children's privacy [36, 120]. This is not wrong, as insecurity is itself a privacy problem worth addressing, but it overlooks the fact that such systems also raise additional privacy issues that need to be addressed.

Other researchers have explored these tensions in their work. For instance, Ghosh et al. [40:1] found that children express frustration with existing parental control apps, finding them "overly restrictive and invasive of their personal privacy, negatively impacting their relationships with their parents." McNally et al. [89] and Badillo-Urquiola et al. [8] conducted participatory design sessions with children and found that children did not wholly eschew parental monitoring and control systems; rather, they sought technologies that helped them learn how to handle challenges and how to seek advice and guidance from parents when they needed it. In other words, the fact that parental control and monitoring systems pose privacy problems (i.e., surveillance, invasion) does not mean that such systems should not exist. It means that researchers and designers need to be intentional about creating such systems in ways that address the privacy and security needs of the children they are intended to protect.

While we used Solove's taxonomy [127] to consider design tensions, researchers could also draw on Dourish and Anderson's socio-cultural approach to privacy [26], Nissenbaum's contextual integrity framework [94], Mulligan et al.'s analytic mapping of privacy dimensions [92], and various approaches to privacy-by-design [151]. We champion these approaches to privacy and security but recognize that they can be hard to grasp for those not already steeped in privacy or sociotechnical system theory. For introductions to some of these frameworks as well as overviews of how privacy affects different domains and user groups, researchers can consult Knijnenburg et al.'s edited collection, *Modern Socio-Technical Perspectives on Privacy* [63], particularly the chapter on privacy in adolescence. Researchers can also draw on a variety of child-specific frameworks pertaining to privacy and security, including Wisniewski et al.'s Teen Online Safety Strategy framework [147], which can also apply to younger children [89], Knowles et al.'s guiding questions to mitigate risk in children's IoT devices [64], Yip et al.'s conceptual model of creepiness in children's technologies [159], and Kumar & Byrne's 5Ds of privacy literacy [66]. As designing for children's privacy and security expands, we encourage researchers to not only draw on these theories and frameworks to strengthen their work, but also to synthesize their insights into theoretical contributions that define the value and worth of this growing design space.

5.2 Bring Children into the Process of Designing for Privacy and Security

As demonstrated by research in our corpus on designing parental monitoring and control systems [8, 40, 89], one avenue that researchers can use to work through the tensions of multiple privacy problems is by engaging children in the design process and centering their perspectives when making design decisions. The guiding questions in Table 2 ask researchers to identify what insights, skills, and capabilities children can contribute to projects and to consider how their work can strengthen children. We acknowledge that conducting research with children presents challenges. It requires expertise in theories as well as research and design methods for working with children, more steps to obtain research ethics approval, and additional efforts related to recruitment or logistics. This process includes tradeoffs, and we encourage researchers to discuss their choices in their publications. For instance, Lindberg et al. [75] conducted most of their design workshops with children from their user population—children with chronic illnesses—but some with non-ill children to avoid overburdening their participants. Wadley et al. [143] designed a system to support hospitalized children but, given the ethical and safety challenges of conducting design workshops with this population, they only worked with parents, teachers, and professional caregivers. They recognized that doing so could bias their work toward adult perspectives and centered children's concerns in their analysis.

Our corpus also contains examples of papers that centered children's perspectives by incorporating already existing materials created by children: Ghosh et al. [40] analyzed online reviews written by children, while Hartikainen et al. [44] included online posts written by children in their analysis of online safety discourse. We recognize that using publicly available information for research presents its own ethical challenges [141], which researchers must address. But we also invite researchers to be creative when considering how to incorporate children's perspectives into their work.

5.3 Adopt an Asset-Based Approach toward Designing for Children's Privacy and Security

Involving children when designing for children's privacy and security embodies the tenets of user-centered design. But we contend that to truly center the interests of children when designing for privacy and security, researchers need to go further than user-centered design and adopt an asset-based approach [153–155]. In this approach, which is commonly emphasized in community development research [65, 88], all community members are considered contributors to community efforts, regardless of age, socio-economic status, or other characteristics. Factors commonly considered as limitations (e.g., special needs, health issues) are leveraged as resources (e.g., people who have gone through health issues can better help others with health issues) [43]. An asset-based approach to children's privacy and security would focus on the skills and resources children have for navigating their privacy and security [134] and how designers can support their development.

Returning to the example of parental control and monitoring systems, some research teams in our corpus that designed parental control or monitoring systems motivated the need for such systems by noting the lack of knowledge among children and parents about risks and how to address them [36, 120]. However, another team studied parents' perceptions of various parental control and monitoring devices and found that parents balance their information needs with their beliefs and values surrounding privacy and the parent-child relationship when deciding whether and how to use such technologies [70]. And teams that conducted participatory design with children regarding parental control and monitoring systems found that children wanted systems to focus on developing children's skills, rather than transmit information to parents [8, 89]. An asset-based approach would treat privacy and security as something that adults can help children themselves accomplish, rather than something that adults need to protect for children.

Key to asset-based approaches is that they are driven by communities themselves, with community members empowered to take action [65, 88]. When applied to designing for children's privacy and security, this means working with specific communities of children on addressing the privacy and security problems *they prioritize* and having *them lead* the development of solutions. Indeed, participatory design researchers have found that, even as children's cognitive, social, and emotional abilities are developing, they are capable of meaningfully engaging in design, provided that researchers employ the appropriate methods to elicit their views [117]. If designers align asset-based approaches with participatory design methods and ground their work in privacy frameworks like Solove's taxonomy [127], they can design for children's privacy and security in a way that centers the interests of children.

6 CONCLUSION

Privacy and security are multifaceted, context-specific concepts that are challenging to design for. By analyzing a corpus of 90 HCI publications related to designing for children's privacy and security, we have found that research addresses a range of privacy problems at several levels, but that there are opportunities to better engage with and center children in this work. Based on our analysis, we advocate that researchers use existing theoretical frameworks to sharpen their privacy and security contributions, and that they adopt an asset-based approach to truly center children. We believe this will lead to designs that equip children to navigate privacy and security challenges, rather than simply protect them from risk.

SELECTION AND PARTICIPATION OF CHILDREN

No children participated in this work.

ACKNOWLEDGMENTS

We thank Rachel Gammons, Nedelina Tchangalova, Lindsay Inge Carpenter, and Jodi Coalter from the University of Maryland Libraries for their assistance in developing the search strategy. We also thank Beth Bonsignore, Emma Dixon, Naeemul Hassan, Pramod Chundury, Xin Qian, Jason Yip, and Michael Cutulle for their feedback on early drafts of this paper. Finally, we thank the anonymous reviewers for their useful insights. This project was funded by the National Science Foundation under two awards: 1951688 and 1951311. No one from the NSF was involved in this research.

REFERENCES

[1] 5Rights Foundation. 2022. *Approaches to children's data protection: A comparative international mapping*. 5Rights Foundation. Retrieved from https://5rightsfoundation.com/Approaches-to-Childrens-Data-Protection---.pdf

[2] Dilrukshi Abeyrathne, Yukihiro Morisawa, Chamari Edirisinghe, Nimesha Ranasinghe, Kasun Karunanayaka, Kening Zhu, Roshan Lalintha Peiris, Owen Noel Newton Fernando, Adrian David Cheok, and Lan Lan. 2011. Connected online and offline safe social networking for children. *Computers in Entertainment* 9, 2: 1–8. https://doi.org/10.1145/1998376.1998380

[3] 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: 1–28. https://doi.org/10.1145/3512904

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

[5] Alissa Antle, Juan Pablo Hourcade, Paulo Blikstein, Jerry Alan Fails, Franca Garzotto, Ole Sejer Iversen, Panos Markopoulos, and Glenda Revelle. 2020. Child-Computer Interaction SIG: Looking Forward After 18 Years. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–4. https://doi.org/10.1145/3334480.3381060

[6] Noah Apthorpe, Sarah Varghese, and Nick Feamster. 2019. Evaluating the Contextual Integrity of Privacy Regulation: Parents' IoT Toy Privacy Norms Versus {COPPA}. In *28th USENIX Security Symposium*, 123–140. Retrieved from https://www.usenix.org/conference/usenixsecurity19/presentation/apthorpe

[7] Ovidiu-Gabriel Baciu-Ureche, Carlie Sleeman, William C. Moody, and Suzanne J. Matthews. 2019. The Adventures of ScriptKitty: Using the Raspberry Pi to Teach Adolescents about Internet Safety. In *Proceedings of the 20th Annual SIG Conference on Information Technology Education*, 118–123. https://doi.org/10.1145/3349266.3351399

[8] 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 Interaction Design and Children on ZZZ - IDC '19*, 394–406. https://doi.org/10.1145/3311927.3323133

[9] Veronica Barassi. 2020. *Child data citizen: how tech companies are profiling us from before birth*. The MIT Press, Cambridge, Massachusetts.

[10] Louise Barkhuus. 2012. The Mismeasurement of Privacy: Using Contextual Integrity to Reconsider Privacy in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '12), 367–376. https://doi.org/10.1145/2207676.2207727

[11] Suzanne Bernstein, Miles Light, and Lauren Merk. 2022. *Policy Brief: A Comparison of Federal Child Privacy Bills*. Future of Privacy Forum, Washington, DC.

Retrieved from https://fpf.org/wp-content/uploads/2022/09/FPF-Policy-Brief-Child-Privacy-Federal-Bill-Comparison-R8.pdf

[12] Ravi Bhoraskar, Seungyeop Han, Jinseong Jeon, Tanzirul Azim, Shuo Chen, Jaeyeon Jung, Suman Nath, Rui Wang, and David Wetherall. 2014. Brahmastra: Driving Apps to Test the Security of Third-Party Components. In *23rd USENIX Security Symposium*, 1021–1036. Retrieved from https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/bhoraskar

[13] 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 Interaction Design and Children Conference - IDC'19*, 439–445. https://doi.org/10.1145/3311927.3325324

[14] Glenn A. Bowen. 2009. Document Analysis as a Qualitative Research Method. *Qualitative Research Journal* 9, 2: 27–40. https://doi.org/10.3316/QRJ0902027

[15] Alex Bowyer, Kyle Montague, Stuart Wheater, Ruth McGovern, Raghu Lingam, and Madeline Balaam. 2018. Understanding the Family Perspective on the Storage, Sharing and Handling of Family Civic Data. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 1–13. https://doi.org/10.1145/3173574.3173710

[16] Ankur Chattopadhyay, David Christian, Adam Ulman, and Caleb Sawyer. 2018. A Middle-School Case Study: Piloting A Novel Visual Privacy Themed Module for Teaching Societal and Human Security Topics Using Social Media Apps. In *2018 IEEE Frontiers in Education Conference (FIE)*, 1–8. https://doi.org/10.1109/FIE.2018.8659278

[17] Parmit K. Chilana, Amy J. Ko, and Jacob Wobbrock. 2015. From User-Centered to Adoption-Centered Design: A Case Study of an HCI Research Innovation Becoming a Product. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*, 1749–1758. https://doi.org/10.1145/2702123.2702412

[18] Jasper Cole, Greg Walsh, and Zach Pease. 2017. Click to Enter: Comparing Graphical and Textual Passwords for Children. In *Proceedings of the 2017 Conference on Interaction Design and Children - IDC '17*, 472–477. https://doi.org/10.1145/3078072.3084311

[19] Lorrie Faith Cranor and Simson Garfinkel (eds.). 2005. *Security and usability: designing secure systems that people can use*. O'Reilly, Beijing; Sebastapol, CA.

[20] Madhurima Das, Gillian Roeder, Anastasia K. Ostrowski, Maria C. Yang, and Aditi Verma. 2023. What Do We Mean When We Write About Ethics, Equity, and Justice in Engineering Design? *Journal of Mechanical Design* 145, 6: 061402. https://doi.org/10.1115/1.4057056

[21] Marijke De Veirman, Liselot Hudders, and Michelle R. Nelson. 2019. What Is Influencer Marketing and How Does It Target Children? A Review and Direction for Future Research. *Frontiers in Psychology* 10. Retrieved January 20, 2023 from https://www.frontiersin.org/articles/10.3389/fpsyg.2019.02685

[22] Leonardo D'Errico, Fabio Franchi, Fabio Graziosi, Claudia Rinaldi, and Francesco Tarquini. 2017. Design and implementation of a children safety system based on IoT technologies. In *2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech)*, 1–6.

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

[24] Digital Futures Commission. 2022. *Problems with data governance in UK schools: the cases of Google Classroom and ClassDojo*. Digital Futures Commission. Retrieved from https://digitalfuturescommission.org.uk/wp-content/uploads/2022/08/Problems-with-data-governance-in-UK-schools.pdf

[25] Kees Dorst. 2015. *Frame Innovation: Create New Thinking by Design*. The MIT Press. https://doi.org/10.7551/mitpress/10096.001.0001

[26] Paul Dourish and Ken Anderson. 2006. Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. *Human-Computer Interaction* 21, 3: 319–342. https://doi.org/10.1207/s15327051hci2103_2

[27] Liz Dowthwaite, Helen Creswick, Virginia Portillo, Jun Zhao, Menisha Patel, Elvira Perez Vallejos, Ansgar Koene, and Marina Jirotka. 2020. "It's your private information. it's your life.": young people's views of personal data use by online technologies. In *Proceedings of the Interaction Design and Children Conference*, 121–134. https://doi.org/10.1145/3392063.3394410

[28] Allison Druin. 2002. The role of children in the design of new technology. *Behaviour & Information Technology* 21, 1: 1–25. https://doi.org/10.1080/01449290110108659

[29] 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* (CHI '21), 1–15. https://doi.org/10.1145/3411764.3445599

[30] Mari Ervasti, Minna Isomursu, and Marianne Kinnula. 2009. Bringing technology into school: NFC-enabled school attendance supervision. In *Proceedings of the 8th International Conference on Mobile and Ubiquitous Multimedia - MUM '09*, 1–10. https://doi.org/10.1145/1658550.1658554

[31] Mari Ervasti, Juhani Laitakari, and Mika Hillukkala. 2016. 'I want to know where my child is at all times' – field study of a location-aware safety service for schoolchildren. *Behaviour & Information Technology* 35, 10: 833–852. https://doi.org/10.1080/0144929X.2016.1201144

[32] Federal Trade Commission. 1998. *Children's Online Privacy Protection Rule ("COPPA")*. Retrieved January 19, 2018 from https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

[33] Michela Ferron, Chiara Leonardi, Paolo Massa, Gianluca Schiavo, Amy L. Murphy, and Elisabetta Farella. 2019. A Walk on the Child Side: Investigating Parents' and Children's Experience and Perspective on Mobile Technology for Outdoor Child Independent Mobility. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*, 1–12. https://doi.org/10.1145/3290605.3300827

[34] Jodi Forlizzi. 2018. Moving beyond user-centered design. *Interactions* 25, 5: 22–23. https://doi.org/10.1145/3239558

[35] Forum on Education Statistics. 2002. Technology in Schools: Suggestions, Tools, and Guidelines for Assessing Technology in Elementary and Secondary Education-Home Page. U.S. Department of Education, Washington, DC. Retrieved from https://nces.ed.gov/pubs2003/tech_schools/

[36] Walter Fuertes, Karina Quimbiulco, Fernando Galarraga, and Jose Luis Garcia-Dorado. 2015. On the Development of Advanced Parental Control Tools. In *2015 1st International Conference on Software Security and Assurance (ICSSA)*, 1–6. https://doi.org/10.1109/ICSSA.2015.011

[37] S.M. Furnell, P. Bryant, and A.D. Phippen. 2007. Assessing the security perceptions of personal Internet users. *Computers & Security* 26, 5: 410–417. https://doi.org/10.1016/j.cose.2007.03.001

[38] Andrew Garbett, David Chatting, Gerard Wilkinson, Clement Lee, and Ahmed Kharrufa. 2018. ThinkActive: Designing for Pseudonymous Activity Tracking in the Classroom. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 1–13. https://doi.org/10.1145/3173574.3173581

[39] William Gaver. 2014. Science and Design: The Implications of Different Forms of Accountability. In *Ways of knowing in HCI*, Judith S. Olson and Wendy Kellogg (eds.). Springer, New York, 143–166.

[40] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J. LaViola Jr, and Pamela J. Wisniewski. 2018. Safety vs. Surveillance: What Children Have to Say about Mobile Apps for Parental Control. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 1–14. https://doi.org/10.1145/3173574.3173698

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

[42] Christina Harrington, Sheena Erete, and Anne Marie Piper. 2019. Deconstructing Community-Based Collaborative Design: Towards More Equitable Participatory Design Engagements. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW: 1–25. https://doi.org/10.1145/3359318

[43] Rebecca Harrison, Christian Blickem, Jonathan Lamb, Susan Kirk, and Ivaylo Vassilev. 2019. Asset-Based Community Development: Narratives, Practice, and Conditions of Possibility—A Qualitative Study With Community Practitioners. *SAGE Open* 9, 1: 2158244018823081. https://doi.org/10.1177/2158244018823081

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

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

[46] Guido van Heck, Itamar Sharon, Paulus Kampert, and Jan van den Berg. 2009. Introducing Electronic Child Records: Balancing Personal Interests, System Performance, and Social Values. In *2009 International Conference on Computational Science and Engineering*, 568–575. https://doi.org/10.1109/CSE.2009.42

[47] Yasamin Heshmat, Carman Neustaedter, and Brendan DeBrincat. 2017. The Autobiographical Design and Long Term Usage of an Always-On Video Recording System for the Home. In *Proceedings of the 2017 Conference on Designing Interactive Systems*, 675–687. https://doi.org/10.1145/3064663.3064759

[48] Sally Holland, Emma Renold, Nicola J. Ross, and Alexandra Hillman. 2010. Power, agency and participatory agendas: A critical exploration of young people's engagement in participative qualitative research. *Childhood* 17, 3: 360–375. https://doi.org/10.1177/0907568210369310

[49] Juan Pablo Hourcade. 2015. *Child-Computer Interaction*. Self-published, Iowa City, IA.

[50] Juan Pablo Hourcade, Glenda Revelle, Anja Zeising, Ole Sejer Iversen, Narcis Pares, Tilde Bekker, and Janet C. Read. 2016. Child-Computer Interaction SIG: New Challenges and Opportunities. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, 1123–1126. https://doi.org/10.1145/2851581.2886433

[51] Juan Pablo Hourcade, Anja Zeising, Ole Sejer Iversen, Narcis Pares, Michael Eisenberg, Chris Quintana, and Mikael B. Skov. 2017. Child-Computer Interaction SIG: Ethics and Values. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, 1334–1337. https://doi.org/10.1145/3027063.3049286

[52] Human Rights Watch. 2022. "How dare they peep into my private life?": Children's rights violations by governments that endorsed online learning during the covid-19 pandemic. Human Rights Watch, New York, NY. Retrieved from https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

[53] Kalpana Hundlani, Sonia Chiasson, and Larry Hamid. 2017. No passwords needed: the iterative design of a parent-child authentication mechanism. In *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services - MobileHCI '17*, 1–11. https://doi.org/10.1145/3098279.3098550

[54] Information Commissioners Office. 2020. *Age appropriate design: A code of practice for online services*. U.K. Information Commissioners Office, Wilmslow, Cheshire, UK. Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/

[55] Ole Sejer Iversen, Rachel Charlotte Smith, and Christian Dindler. 2017. Child as Protagonist: Expanding the Role of Children in Participatory Design. In *Proceedings of the 2017 Conference on Interaction Design and Children*, 27–37. https://doi.org/10.1145/3078072.3079725

[56] Saba Kawas, Ye Yuan, Akeiylah DeWitt, Qiao Jin, Susanne Kirchner, Abigail Bilger, Ethan Grantham, Julie A Kientz, Andrea Tartaro, and Svetlana Yarosh. 2020. Another decade of IDC research: examining and reflecting on values and ethics. In *Proceedings of the Interaction Design and Children Conference*, 205–215. https://doi.org/10.1145/3392063.3394436

[57] Chrisovalantis Kefalidis, Georgia Lazakidou, and Symeon Retalis. 2009. SyCo: a collaborative learning tool for generating ideas in private and in public. In *Proceedings of the 8th International Conference on Interaction Design and Children - IDC '09*, 162. https://doi.org/10.1145/1551788.1551817

[58] Girard Kelly, Jeff Graham, Jill Bronfman, and Steve Garton. 2021. *Privacy of streaming apps and devices: Watching TV that watches us*. Common Sense Media, San Francisco, CA. Retrieved from https://www.commonsensemedia.org/sites/default/files/research/report/privacy_of_streaming_apps_and_devices-final.pdf

[59] Girard Kelly, Jeff Graham, Jill Bronfman, and Steve Garton. 2021. *2021 state of kids' privacy*. Common Sense Media, San Francisco, CA. Retrieved from https://www.commonsensemedia.org/sites/default/files/research/report/common-sense-2021-state-of-kids-privacy_0.pdf

[60] Girard Kelly, Jeff Graham, Jill Bronfman, and Steve Garton. 2022. *Privacy of virtual reality: Our future in the metaverse and beyond*. Common Sense Media, San Francisco, CA. Retrieved from https://www.commonsensemedia.org/sites/default/files/research/report/privacy-of-virtual-reality-our-future-in-the-metaverse-and-beyond.pdf

[61] Marianne Kinnula, Netta Iivari, Minna Isomursu, and Henrietta Kinnula. 2018. Socializers, achievers or both? Value-based roles of children in technology design projects. *International Journal of Child-Computer Interaction* 17: 39–49. https://doi.org/10.1016/j.ijcci.2018.04.004

[62] Marianne Kinnula, Netta Iivari, Tonja Molin-Juustila, Eino Keskitalo, Topi Leinonen, Eetu Mansikkamäki, Toni Käkelä, and Martti Similä. 2017. Cooperation, Combat, or Competence Building – What Do We Mean When We Are 'Empowering Children' in and through Digital Technology Design? *ICIS 2017 Proceedings*. Retrieved from https://aisel.aisnet.org/icis2017/TransformingSociety/Presentations/15

[63] Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano (eds.). 2021. *Modern socio-technical perspectives on Privivacy*. Springer Naturre, Gewerbestrasse, Switzerland.

[64] Bran Knowles, Sophie Beck, Joe Finney, James Devine, and Joseph Lindley. 2019. A Scenario-Based Methodology for Exploring Risks: Children and Programmable IoT. In *Proceedings of the 2019 on Designing Interactive Systems Conference - DIS '19*, 751–761. https://doi.org/10.1145/3322276.3322315

[65] John Kretzmann and John P. McKnight. 1996. Assets-based community development. *National Civic Review* 85, 4: 23–29. https://doi.org/10.1002/ncr.4100850405

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

[67] Priya C. Kumar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2019. Privacy and security considerations for digital technology use in elementary schools. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*, 1–13. https://doi.org/10.1145/3290605.3300537

[68] 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: 1–21. https://doi.org/10.1145/3134699

[69] 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)*, 67–79. https://doi.org/10.1145/3202185.3202735

[70] Anastasia Kuzminykh and Edward Lank. 2019. How Much is Too Much?: Understanding the Information Needs of Parents of Young Children. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3, 2: 1–21. https://doi.org/10.1145/3328923

[71] Elizabeth Laird, Hugh Grant-Chapman, Cody Venzke, and Hannah Quay-de la Vallee. 2022. *Hidden Harms: The Misleading Promise of Monitoring Students Online*. Center for Democracy and Technology, Washington, DC. Retrieved from https://cdt.org/wp-content/uploads/2022/08/Hidden-Harms-The-Misleading-Promise-of-Monitoring-Students-Online-Research-Report-Final-Accessible.pdf

[72] Elmer Lastdrager, Inés Carvajal Gallardo, Pieter Hartel, and Marianne Junger. 2017. How Effective is Anti-Phishing Training for Children? In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 229–239. Retrieved from https://www.usenix.org/system/files/conference/soups2017/soups2017-lastdrager.pdf

[73] Iolanda Leite and Jill Fain Lehman. 2016. The Robot Who Knew Too Much: Toward Understanding the Privacy/Personalization Trade-Off in Child-Robot Conversation. In *Proceedings of the The 15th International Conference on Interaction Design and Children - IDC '16*, 379–387. https://doi.org/10.1145/2930674.2930687

[74] Ilaria Liccardi, Monica Bulger, Hal Abelson, Daniel J. Weitzner, and Wendy Mackay. 2014. Can apps play by the COPPA Rules? In *2014 Twelfth Annual International Conference on Privacy, Security and Trust*, 1–9. https://doi.org/10.1109/PST.2014.6890917

[75] Susanne Lindberg, Pontus Wärnestål, Jens Nygren, and Petra Svedberg. 2014. Designing digital peer support for children: design patterns for social interaction. In *Proceedings of the 2014 conference on Interaction design and children - IDC '14*, 47–56. https://doi.org/10.1145/2593968.2593972

[76] Minxing Liu, Haoyu Wang, Yao Guo, and Jason Hong. 2016. Identifying and Analyzing the Privacy of Apps for Kids. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications - HotMobile '16*, 105–110. https://doi.org/10.1145/2873587.2873597

[77] Sonia Livingstone. 2003. Children's Use of the Internet: Reflections on the Emerging Research Agenda. *New Media & Society* 5, 2: 147–166. https://doi.org/10.1177/1461444803005002001

[78] Sonia Livingstone. 2006. Children's Privacy Online: Experimenting with Boundaries Within and Beyond the Family. In *Computers, Phones, and the Internet: Domesticating Information Technology*, Robert Kraut, Malcolm Brynin and Sara Kiesler (eds.). Oxford University Press, New York, NY, 145–167.

[79] Sonia Livingstone. 2018. Children: A Special Case for Privacy. *InterMedia 46*, 18–23.

[80] Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri. 2018. *Children's data and privacy online*. London School of Economics, London. Retrieved from http://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf

[81] Deborah Lupton and Ben Williamson. 2017. The datafied child: The dataveillance of children and implications for their rights. *New Media & Society* 19, 5: 780–794. https://doi.org/10.1177/1461444816686328

[82] Sus Lyckvi and Olof Torgersson. 2018. Privacy and design ethics vs designing for curiosity, communication and children: lessons learned. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services - MobileHCI '18*, 1–8. https://doi.org/10.1145/3229434.3229480

[83] Sapna Maheshwari. 2018. Oath Agrees to $5 Million Settlement Over Children's Privacy Online. *The New York Times*. Retrieved September 4, 2019 from https://www.nytimes.com/2018/12/03/business/media/oath-children-online-privacy.html

[84] Sana Maqsood and Sonia Chiasson. 2021. "They think it's totally fine to talk to somebody on the internet they don't know": Teachers' perceptions and mitigation strategies of tweens' online risks. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–17. https://doi.org/10.1145/3411764.3445224

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

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

[87] Giovanna Mascheroni and Andra Siibak. 2021. *Datafied Childhoods*. Peter Lang US. https://doi.org/10.3726/b17460

[88] Alison Mathie and Gord Cunningham. 2003. From clients to citizens: Asset-based Community Development as a strategy for community-driven development. *Development in Practice* 13, 5: 474–486. https://doi.org/10.1080/0961452032000125857

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

[90] 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*, 5197–5207. https://doi.org/10.1145/3025453.3025735

[91] Carol Moser, Tianying Chen, and Sarita Y. Schoenebeck. 2017. Parents' and Children's Preferences about Parents Sharing about Children on Social Media. 5221–5225. https://doi.org/10.1145/3025453.3025587

[92] Deirdre K. Mulligan, Colin Koopman, and Nick Doty. 2016. Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374, 2083: 1–17. https://doi.org/10.1098/rsta.2016.0118

[93] Fnu Nazneen, Fatima A. Boujarwah, Shone Sadler, Amha Mogus, Gregory D. Abowd, and Rosa I. Arriaga. 2010. Understanding the challenges and opportunities for richer descriptions of stereotypical behaviors of children with asd: a concept exploration and validation. In *Proceedings of the 12th international ACM SIGACCESS conference on Computers and accessibility - ASSETS '10*, 67. https://doi.org/10.1145/1878803.1878817

[94] Helen Nissenbaum. 2010. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, Stanford, CA.

[95] Jason Nolan, Kate Raynes-Goldie, and Melanie McBride. 2011. The Stranger Danger: Exploring Surveillance, Autonomy, and Privacy in Children's Use of Social Media. *Journal of Childhood Studies* 36, 2: 24–32. https://doi.org/10.18357/jcs.v36i2.15089

[96] Marije Nouwen, Selina Schepers, Karen Mouws, Karin Slegers, Niek Kosten, and Pieter Duysburgh. 2016. Designing an educational music game: What if children were calling the tune? *International Journal of Child-Computer Interaction* 9–10: 20–32. https://doi.org/10.1016/j.ijcci.2016.10.001

[97] Carly Nyst, Amaya Gorostiaga, and Patrick Geary. 2018. *Industry Toolkit: Children's Online Privacy and Freedom of Expression*. UNICEF. Retrieved from https://sites.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf

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

[99] Ofcom. 2022. *Children and parents: Media use and attitudes report 2022*. Ofcom, London, UK. Retrieved from https://www.ofcom.org.uk/__data/assets/pdf_file/0024/234609/childrens-media-use-and-attitudes-report-2022.pdf

[100] Office of Educational Technology. 2017. *Reimagining the Role of Technology in Education: 2017 National Education Technology Plan Update*. U.S. Department of Education, Washington, DC. Retrieved from https://tech.ed.gov/files/2017/01/NETP17.pdf

[101] Marc Olano, Alan Sherman, Linda Oliva, Ryan Cox, Deborah Firestone, Oliver Kubik, Milind Patil, John Seymour, Isaac Sohn, and Donna Thomas. 2014. SecurityEmpire: Development and Evaluation of a Digital Game to Promote Cybersecurity Education. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*. Retrieved January 24, 2023 from https://www.usenix.org/conference/3gse14/summit-program/presentation/olano

[102] Anastasia K. Ostrowski, Raechel Walker, Madhurima Das, Maria Yang, Cynthia Breazea, Hae Won Park, and Aditi Verma. 2022. Ethics, Equity, & Justice in Human-Robot Interaction: A Review and Future Directions. In *2022 31st IEEE International Conference on Robot and Human Interactive Communication (RO-MAN)*, 969–976. https://doi.org/10.1109/RO-MAN53752.2022.9900805

[103] Leysia Palen and Paul Dourish. 2003. Unpacking "Privacy" for a Networked World. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '03), 129–136. https://doi.org/10.1145/642611.642635

[104] Lyta Penna, Andrew Clark, and George Mohay. 2010. A Framework for Improved Adolescent and Child Safety in MMOs. In *2010 International Conference on Advances in Social Networks Analysis and Mining*, 33–40. https://doi.org/10.1109/ASONAM.2010.66

[105] Sandra Petronio. 2002. *Boundaries of privacy: dialectics of disclosure*. State University of New York Press, Albany, NY.

[106] 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*, 352–357. https://doi.org/10.1145/3078072.3079722

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

[108] Noor Hayani Abd Rahim, Suraya Hamid, Miss Laiha Mat Kiah, Shahaboddin Shamshirband, and Steven Furnell. 2015. A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes* 44, 4: 606–622. https://doi.org/10.1108/K-12-2014-0283

[109] Jyri Rajamaki, Paresh Rathod, Anu Ahlgren, Johanna Aho, Mari Takari, and Sami Ahlgren. 2012. Resilience of Cyber-Physical System: A Case Study of Safe School Environment. In *2012 European Intelligence and Security Informatics Conference*, 285–285. https://doi.org/10.1109/EISIC.2012.10

[110] Janet C. Read and Russell Beale. 2009. Under My Pillow: Designing Security for Children's Special Things. In *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology* (BCS-HCI '09), 288–292. Retrieved August 29, 2019 from http://dl.acm.org/citation.cfm?id$=$1671011.1671046

[111] Janet C. Read and Mathilde M. Bekker. 2011. The Nature of Child Computer Interaction. https://doi.org/10.14236/ewic/HCI2011.43

[112] 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 - IDC '12*, 200. https://doi.org/10.1145/2307096.2307125

[113] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman. 2018. "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. *Proceedings on Privacy Enhancing Technologies* 2018, 3: 63–83. https://doi.org/10.1515/popets-2018-0021

[114] Victoria Rideout and Michael B. Robb. 2020. *The Common Sense census: Media use by kids age zero to eight, 2020*. Common Sense Media, San Francisco, CA. Retrieved from https://www.commonsensemedia.org/sites/default/files/research/report/2020_zero_to_eight_census_final_web.pdf

[115] Victoria Rideout and Michael B. Robb. 2022. *Common Sense census: Media use by tweens and teens, 2021*. Common Sense Media, San Francisco, CA. Retrieved from https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf

[116] Jennifer A. Rode. 2009. Digital Parenting: Designing Children's Safety. In *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers*, 244–251.

[117] Yvonne Rogers, Chris Frauenberger, and Chris Quintana. 2017. Conversation: Tensions and Possibilities between Learning and Participatory Design. In *Participatory design for learning*, Betsy DiSalvo, Jason Yip, Elizabeth Bonsignore and Carl DiSalvo (eds.). Routledge, Taylor & Francis Group, New York, 225–234.

[118] Johnny Saldaña. 2013. *The coding manual for qualitative researchers*. SAGE, Los Angeles.

[119] Spyridon Samonas and David Coss. 2014. The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security* 10, 3: 21–45.

[120] Phakpoom Santisarun and Sirapat Boonkrong. 2015. Social network monitoring application for parents with children under thirteen. In *2015 7th International Conference on Knowledge and Smart Technology (KST)*, 75–80. https://doi.org/10.1109/KST.2015.7051456

[121] Selina Schepers, Katrien Dreessen, and Bieke Zaman. 2018. Rethinking children's roles in Participatory Design: The child as a process designer. *International Journal of Child-Computer Interaction* 16: 47–54. https://doi.org/10.1016/j.ijcci.2017.12.001

[122] Donald A. Schön. 2016. *The reflective practitioner: how professionals think in action*. Routledge, London.

[123] Helen Sharp, Jenny Preece, and Yvonne Rogers. 2019. *Interaction design: beyond human-computer interaction*. John Wiley & Sons, Inc, Indianapolis, IN.

[124] Natasha Singer. 2017. How Google Took Over the Classroom. *The New York Times*. Retrieved May 19, 2017 from https://www.nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html

[125] H. Jeff Smith, Tamara Dinev, and Heng Xu. 2011. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly* 35, 4: 980–1015.

[126] Kiley Sobel, Arpita Bhattacharya, Alexis Hiniker, Jin Ha Lee, Julie A. Kientz, and Jason C. Yip. 2017. It wasn't really about the Pokémon: Parents' Perspectives on a Location-Based Mobile Game. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 1483–1496. https://doi.org/10.1145/3025453.3025761

[127] Daniel Solove. 2008. *Understanding Privacy*. Harvard University Press, Cambridge, Massachusetts.

[128] Katta Spiel, Christopher Frauenberger, Os Keyes, and Geraldine Fitzpatrick. 2019. Agency of Autistic Children in Technology Research—A Critical Literature Review. *ACM Transactions on Computer-Human Interaction* 26, 6: 1–40. https://doi.org/10.1145/3344919

[129] Katta Spiel, Kathrin Gerling, Cynthia L. Bennett, Emeline Brulé, Rua M. Williams, Jennifer Rode, and Jennifer Mankoff. 2020. Nothing About Us Without Us: Investigating the Role of Critical Disability Studies in HCI. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–8. https://doi.org/10.1145/3334480.3375150

[130] Valerie Steeves. 2010. *Summary of Research on Youth Online Privacy*. Office of the Privacy Commissioner of Canada, Ottawa, Canada. Retrieved from https://priv.gc.ca/media/1731/yp_201003_e.pdf

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

[132] Mariya Stoilova, Rishita Nandagiri, and Sonia Livingstone. 2019. Children's understanding of personal data and privacy online—A systematic evidence mapping. *Information, Communication & Society*: 1–19. https://doi.org/10.1080/1369118X.2019.1657164

[133] Joshua Streiff, Olivia Kenny, Sanchari Das, Andrew Leeth, and L. Jean Camp. 2018. Poster Abstract: Who's Watching Your Child? Exploring Home Security Risks with Smart Toy Bears. In *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 285–286. https://doi.org/10.1109/IoTDI.2018.00042

[134] Mega Subramaniam, Priya Kumar, Shandra Morehouse, Yuting Liao, and Jessica Vitak. 2019. Leveraging funds of knowledge to manage privacy practices in families. *Proceedings of the Association for Information Science and Technology (ASIS&T '19)* 56, 1: 245–254. https://doi.org/10.1002/pra2.67

[135] Sangho Suh, Sydney Lamorea, Edith Law, and Leah Zhang-Kennedy. 2022. PrivacyToon: Concept-driven Storytelling with Creativity Support for Privacy Concepts. In *Designing Interactive Systems Conference*, 41–57. https://doi.org/10.1145/3532106.3533557

[136] Kaiwen Sun, Yixin Zou, Jenny Radesky, Christopher Brooks, and Florian Schaub. 2021. Child Safety in the Smart Home: Parents' Perceptions, Needs, and Mitigation Strategies. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2: 1–41. https://doi.org/10.1145/3479858

[137] Andreas Tsirtsis, Nicolas Tsapatsoulis, Makis Stamatelatos, Kwstantinos Papadamou, and Michael Sirivianos. 2016. Cyber security risks for minors: A taxonomy and a software architecture. In *2016 11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP)*, 93–99. https://doi.org/10.1109/SMAP.2016.7753391

[138] Maarten Van Mechelen, Gökçe Elif Baykal, Christian Dindler, Eva Eriksson, and Ole Sejer Iversen. 2020. 18 Years of ethics in child-computer interaction research: a systematic literature review. In *Proceedings of the Interaction Design and Children Conference*, 161–183. https://doi.org/10.1145/3392063.3394407

[139] Maarten Van Mechelen, Line Have Musaeus, Ole Sejer Iversen, Christian Dindler, and Arthur Hjorth. 2021. A Systematic Review of Empowerment in Child-Computer Interaction Research. In *Interaction Design and Children*, 119–130. https://doi.org/10.1145/3459990.3460701

[140] Asimina Vasalou, Anne-Marie Oostveen, and Adam N. Joinson. 2012. A Case Study of Non-adoption: The Values of Location Tracking in the Family. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work* (CSCW '12), 779–788. https://doi.org/10.1145/2145204.2145321

[141] Jessica Vitak, Katie Shilton, and Zahra Ashktorab. 2016. Beyond the Belmont Principles: Ethical Challenges, Practices, and Beliefs in the Online Data Research Community. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing - CSCW '16*, 939–951. https://doi.org/10.1145/2818048.2820078

[142] René Vutborg, Jesper Kjeldskov, Jeni Paay, Sonja Pedell, and Frank Vetere. 2011. Supporting young children's communication with adult relatives across time zones. In *Proceedings of the 23rd Australian Computer-Human Interaction Conference on - OzCHI '11*, 291–300. https://doi.org/10.1145/2071536.2071583

[143] Greg Wadley, Frank Vetere, Liza Hopkins, Julie Green, and Lars Kulik. 2014. Exploring ambient technology for connecting hospitalised children with school and home. *International Journal of Human-Computer Studies* 72, 8–9: 640–653. https://doi.org/10.1016/j.ijhcs.2014.04.003

[144] Ge Wang, Jun Zhao, Max Van Kleek, and Nigel Shadbolt. 2022. "Don't make assumptions about me!": Understanding Children's Perception of Datafication Online. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2: 1–24. https://doi.org/10.1145/3555144

[145] Yang Wang. 2018. Inclusive Security and Privacy. *IEEE Security & Privacy* 16, 4: 82–87. https://doi.org/10.1109/MSP.2018.3111237

[146] Buffy Wicks and Jordan Cunningham. 2022. *The California Age Appropriate Design Code.* California State Assembly, Sacramento, CA. Retrieved from https://5rightsfoundation.com/uploads/California-Age-Appropriate-Design-Code_short-briefing.pdf

[147] Pamela Wisniewski, Arup Kumar Ghosh, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2017. Parental Control vs. Teen Self-Regulation: Is there a middle ground for mobile online safety? In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 51–69. https://doi.org/10.1145/2998181.2998352

[148] Pamela Wisniewski, Heng Xu, John M. Carroll, and Mary Beth Rosson. 2013. Grand Challenges of Researching Adolescent Online Safety: A Family Systems Approach. In *Proceedings of the Nineteenth Americas Conference on Information Systems*, 1–8. Retrieved from https://www.pamspam.com/wp-content/uploads/AMCIS2013_GrandChallenges_Camera.pdf

[149] Maxine Wolfe and Robert Laufer. 1975. The concept of privacy in childhood and adolescence. In *Man-environment interactions: evaluations and applications*, Stephen T. Margulis (ed.). Halsted Press, 29–54.

[150] Julia Carrie Wong. 2019. "It's not play if you're making money": how Instagram and YouTube disrupted child labor laws. *The Guardian*. Retrieved March 17, 2020 from https://www.theguardian.com/media/2019/apr/24/its-not-play-if-youre-making-money-how-instagram-and-youtube-disrupted-child-labor-laws

[151] Richmond Y. Wong and Deirdre K. Mulligan. 2019. Bringing Design to the Privacy Table: Broadening "Design" in "Privacy by Design" Through the Lens of HCI. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*, 1–17. https://doi.org/10.1145/3290605.3300492

[152] Marisol Wong-Villacres and Shaowen Bardzell. 2011. Technology-mediated parent-child intimacy: designing for ecuadorian families separated by migration. In *Proceedings of the 2011 annual conference extended abstracts on Human factors in computing systems - CHI EA '11*, 2215. https://doi.org/10.1145/1979742.1979877

[153] Marisol Wong-Villacres, Sheena Erete, Aakash Gautam, Azra Ismail, Neha Kumar, Lucy Pei, Wendy Roldan, Veronica Ahumada-Newhart, Karla Badillo-Urquiola, J. Maya Hernandez, Anthony Poon, Pedro Reynolds-Cuéllar, and Vivian Genaro Motti. 2022. Elevating strengths and capacities: the different shades of assets-based design in HCI. *Interactions* 29, 5: 28–33. https://doi.org/10.1145/3549068

[154] 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 *Conference Companion Publication of the 2020 on Computer Supported Cooperative Work and Social Computing*, 527–535. https://doi.org/10.1145/3406865.3418594

[155] Marisol Wong-Villacres, Aakash Gautam, Deborah Tatar, and Betsy DiSalvo. 2021. Reflections on Assets-Based Design: A Journey Towards A Collective of Assets-Based Thinkers. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2: 1–32. https://doi.org/10.1145/3479545

[156] Svetlana Yarosh, Yee Chieh "Denise" Chew, and Gregory D. Abowd. 2009. Supporting parent–child communication in divorced families. *International Journal of Human-Computer Studies* 67, 2: 192–203. https://doi.org/10.1016/j.ijhcs.2008.09.005

[157] Svetlana Yarosh, Iulian Radu, Seth Hunter, and Eric Rosenbaum. 2011. Examining values: an analysis of nine years of IDC research. In *Proceedings of the 10th International Conference on Interaction Design and Children - IDC '11*, 136–144. https://doi.org/10.1145/1999030.1999046

[158] Yanfang Ye, Tao Li, and Haiyin Shen. 2015. Soter: Smart Bracelets for Children's Safety. *ACM Transactions on Intelligent Systems and Technology* 6, 4: 1–20. https://doi.org/10.1145/2700483

[159] 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*, 1–15. https://doi.org/10.1145/3290605.3300303

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

[161] Hee Jung Yoon, Ho-Kyeong Ra, Can Basaran, Sang Hyuk Son, Taejoon Park, and Jeonggil Ko. 2017. Fuzzy Bin-Based Classification for Detecting Children's Presence with 3D Depth Cameras. *ACM Transactions on Sensor Networks* 13, 3: 1–28. https://doi.org/10.1145/3079764

[162] 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: 10–18. https://doi.org/10.1016/j.ijcci.2017.05.001

[163] Leah Zhang-Kennedy and Sonia Chiasson. 2022. A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Computing Surveys* 54, 1: 1–39. https://doi.org/10.1145/3427920

[164] 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 15th International Conference on Interaction Design and Children* (IDC '16), 388–399. https://doi.org/10.1145/2930674.2930716

[165] Jun Zhao, Blanche Duron, and Ge Wang. 2022. KOALA Hero: Inform Children of Privacy Risks of Mobile Apps. In *Interaction Design and Children*, 523–528. https://doi.org/10.1145/3501712.3535278

[166] 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*, 1–13. https://doi.org/10.1145/3290605.3300336

[167] Maximilian Zinkus, Oliver Curry, Marina Moore, Zachary Peterson, and Zoë J. Wood. 2019. Fakesbook: A social networking platform for teaching security and privacy concepts to secondary school students. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*, 892–898. https://doi.org/10.1145/3287324.3287486

A Appendix

This appendix lists the 90 publications included in our corpus of HCI research from 2009-2019 related to designing for children's privacy and security.

1. Dilrukshi Abeyrathne, Yukihiro Morisawa, Chamari Edirisinghe, Nimesha Ranasinghe, Kasun Karunanayaka, Kening Zhu, Roshan Lalintha Peiris, Owen Noel Newton Fernando, Adrian David Cheok, and Lan Lan. 2011. Connected online and offline safe social networking for children. *Computers in Entertainment* 9, 2: 1–8. https://doi.org/10.1145/1998376.1998380

2. A.E. Al-Naser and W.M. El-Medany. 2018. Children Safety Using Smartwatch with Anomaly Detection Approach Model. In *Smart Cities Symposium 2018*, 2 (4 pp.)-2 (4 pp.). https://doi.org/10.1049/cp.2018.1370

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

4. Noah Apthorpe, Sarah Varghese, and Nick Feamster. 2019. Evaluating the Contextual Integrity of Privacy Regulation: Parents' IoT Toy Privacy Norms Versus {COPPA}. In *28th USENIX Security Symposium*, 123–140. Retrieved from https://www.usenix.org/conference/usenixsecurity19/presentation/apthorpe

5. 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 Interaction Design and Children on ZZZ - IDC '19*, 394–406. https://doi.org/10.1145/3311927.3323133

6. Ravi Bhoraskar, Seungyeop Han, Jinseong Jeon, Tanzirul Azim, Shuo Chen, Jaeyeon Jung, Suman Nath, Rui Wang, and David Wetherall. 2014. Brahmastra: Driving Apps to Test the Security of Third-Party Components. In *23rd USENIX Security Symposium*, 1021–1036. Retrieved from https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/bhoraskar

7. 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 Interaction Design and Children Conference - IDC'19*, 439–445. https://doi.org/10.1145/3311927.3325324

8. Alex Bowyer, Kyle Montague, Stuart Wheater, Ruth McGovern, Raghu Lingam, and Madeline Balaam. 2018. Understanding the Family Perspective on the Storage, Sharing and Handling of Family Civic Data. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 1–13. https://doi.org/10.1145/3173574.3173710

9. Eva Irene Brooks and Anders Kalsgaard Moeller. 2019. Children's Perceptions and Concerns of Online Privacy. In *Extended Abstracts of the Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts - CHI PLAY '19 Extended Abstracts*, 357–362. https://doi.org/10.1145/3341215.3356307

10. Jasper Cole, Greg Walsh, and Zach Pease. 2017. Click to Enter: Comparing Graphical and Textual Passwords for Children. In *Proceedings of the 2017 Conference on Interaction Design and Children - IDC '17*, 472–477. https://doi.org/10.1145/3078072.3084311

11. Francesco D'Andria, Jose Miguel Garrido, Michael Boniface, Stefano Modafferi, Simon Crowle, Lee Middleton, Konstantinos C. Apostolakis, Kosmas Dimitropoulos, and Petros Daras. 2018. ProsocialLearn: A Prosocial Games Marketplace. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 1–5. https://doi.org/10.1109/NTMS.2018.8328715

12. Leonardo D'Errico, Fabio Franchi, Fabio Graziosi, Claudia Rinaldi, and Francesco Tarquini. 2017. Design and implementation of a children safety system based on IoT technologies. In *2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech)*, 1–6.

13. Mari Ervasti, Minna Isomursu, and Marianne Kinnula. 2009. Bringing technology into school: NFC-enabled school attendance supervision. In *Proceedings of the 8th International Conference on Mobile and Ubiquitous Multimedia - MUM '09*, 1–10. https://doi.org/10.1145/1658550.1658554

14. Mari Ervasti, Juhani Laitakari, and Mika Hillukkala. 2016. 'I want to know where my child is at all times' – field study of a location-aware safety service for schoolchildren. *Behaviour & Information Technology* 35, 10: 833–852. https://doi.org/10.1080/0144929X.2016.1201144

15. Zhiyuan Fang, Li Wei, Wei Chen, and Yangjun He. 2012. A RFID-Based Kindergarten Intelligence Security System. In *2012 IEEE Ninth International Conference on e-Business Engineering*, 321–326. https://doi.org/10.1109/ICEBE.2012.59

16. Michela Ferron, Chiara Leonardi, Paolo Massa, Gianluca Schiavo, Amy L. Murphy, and Elisabetta Farella. 2019. A Walk on the Child Side: Investigating Parents' and Children's Experience and Perspective on Mobile Technology for Outdoor Child Independent Mobility. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*, 1–12. https://doi.org/10.1145/3290605.3300827

17. Walter Fuertes, Karina Quimbiulco, Fernando Galarraga, and Jose Luis Garcia-Dorado. 2015. On the Development of Advanced Parental Control Tools. In *2015 1st International Conference on Software Security and Assurance (ICSSA)*, 1–6. https://doi.org/10.1109/ICSSA.2015.011

18. Masaki Fujikawa, Ryoya Kanou, Airi Itoh, and Yoshie Abe. 2019. Development of an SNS education game for higher-grade elementary school children. In *Proceedings of the 10th International Conference on E-Education, E-Business, E-Management and E-Learning - IC4E '19*, 130–134. https://doi.org/10.1145/3306500.3306501

19. Ganesh Gaikwad and Abhishek Jain. 2017. Feelbot: Reducing Use of Bad Words in Children through Wearable using Artificial Intelligence and Gamification. In *Proceedings of the 2017 Conference on Interaction Design and Children - IDC '17*, 777–781. https://doi.org/10.1145/3078072.3105876

20. Andrew Garbett, David Chatting, Gerard Wilkinson, Clement Lee, and Ahmed Kharrufa. 2018. ThinkActive: Designing for Pseudonymous Activity Tracking in the Classroom. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 1–13. https://doi.org/10.1145/3173574.3173581

21. Christine Geeng and Franziska Roesner. 2019. Who's In Control?: Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*, 1–13. https://doi.org/10.1145/3290605.3300498

22. Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J. LaViola Jr, and Pamela J. Wisniewski. 2018. Safety vs. Surveillance: What Children Have to Say about Mobile Apps for Parental Control. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 1–14. https://doi.org/10.1145/3173574.3173698

23. Stuart Gray, Kirsten Cater, Chloe Meineck, Rachel Hahn, Debbie Watson, and Tom Metcalfe. 2019. Trove: A Digitally Enhanced Memory Box for Looked after and Adopted Children. In *Proceedings of the Interaction Design and Children Conference - IDC '19*, 458–463. https://doi.org/10.1145/3311927.3325305

24. Samir N. Hamade. 2015. Parental Awareness and Mediation of Children's Internet Use in Kuwait. In *2015 12th International Conference on Information Technology - New Generations*, 640–645. https://doi.org/10.1109/ITNG.2015.107

25. Heidi Hartikainen, Netta Iivari, and Marianne Kinnula. 2016. Should We Design for Control, Trust or Involvement?: A Discourses Survey About Children's Online Safety. In *Proceedings of the 15th International Conference on Interaction Design and Children* (IDC '16), 367–378. https://doi.org/10.1145/2930674.2930680

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

27. Guido van Heck, Itamar Sharon, Paulus Kampert, and Jan van den Berg. 2009. Introducing Electronic Child Records: Balancing Personal Interests, System Perfomance, and Social Values. In *2009 International Conference on Computational Science and Engineering*, 568–575. https://doi.org/10.1109/CSE.2009.42

28. Yasamin Heshmat, Carman Neustaedter, and Brendan DeBrincat. 2017. The Autobiographical Design and Long Term Usage of an Always-On Video Recording System for the Home. In *Proceedings of the 2017 Conference on Designing Interactive Systems*, 675–687. https://doi.org/10.1145/3064663.3064759

29. Masayuki Higashino, Tamami Imado, and Masashi Inoue. 2019. Design of a Computerized Educational System about Risks of Social Networking Services for Children. In *Proceedings of the 2019 2nd International Conference on Geoinformatics and Data Analysis*, 89–92. https://doi.org/10.1145/3318236.3318263

30. Mengjia Hu and Xumin Wu. 2018. Research on Children's Network Privacy Protection in Mobile Social Media. In *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 1135–1138. https://doi.org/10.1109/HPCC/SmartCity/DSS.2018.00190

31. Kalpana Hundlani, Sonia Chiasson, and Larry Hamid. 2017. No passwords needed: the iterative design of a parent-child authentication mechanism. In *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services - MobileHCI '17*, 1–11. https://doi.org/10.1145/3098279.3098550

32. Yordanka Karayaneva and Diana Hintea. 2018. Object recognition algorithms implemented on NAO robot for children's visual learning enhancement. In *Proceedings of the 2018 2nd International Conference on Mechatronics Systems and Control Engineering - ICMSCE 2018*, 86–92. https://doi.org/10.1145/3185066.3185083

33. Alex Kayal, M. Birna van Riemsdijk, Mark A. Neerincx, and Willem-Paul Brinkman. 2018. Socially adaptive electronic partners for improved support of children's values: An empirical study with a location-sharing mobile app. *International Journal of Child-Computer Interaction* 18: 79–89. https://doi.org/10.1016/j.ijcci.2018.09.001

34. Chrisovalantis Kefalidis, Georgia Lazakidou, and Symeon Retalis. 2009. SyCo: a collaborative learning tool for generating ideas in private and in public. In *Proceedings of the 8th International Conference on Interaction Design and Children - IDC '09*, 162. https://doi.org/10.1145/1551788.1551817

35. Tae Young Kim and JongBeom Lim. 2018. A Cloud-based Physical Body Data Sensing Architecture for Playing Children. In *2018 1st IEEE International Conference on Knowledge Innovation and Invention (ICKII)*, 120–123. https://doi.org/10.1109/ICKII.2018.8569079

36. Bran Knowles, Sophie Beck, Joe Finney, James Devine, and Joseph Lindley. 2019. A Scenario-Based Methodology for Exploring Risks: Children and Programmable IoT. In *Proceedings of the 2019 on Designing Interactive Systems Conference - DIS '19*, 751–761. https://doi.org/10.1145/3322276.3322315

37. E. Kritzinger. 2015. Enhancing cyber safety awareness among school children in South Africa through gaming. In *2015 Science and Information Conference (SAI)*, 1243–1248. https://doi.org/10.1109/SAI.2015.7237303

38. Priya C. Kumar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2019. Privacy and security considerations for digital technology use in elementary schools. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*, 1–13. https://doi.org/10.1145/3290605.3300537

39. 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)*, 67–79. https://doi.org/10.1145/3202185.3202735

40. Elizabeth Baby Kuriakose. 2019. A Smart Sensor School Management System That Improves Security Of Student. In *2019 International Conference on Fourth Industrial Revolution (ICFIR)*, 1–6. https://doi.org/10.1109/ICFIR.2019.8894773

41. Anastasia Kuzminykh and Edward Lank. 2019. How Much is Too Much?: Understanding the Information Needs of Parents of Young Children. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3, 2: 1–21. https://doi.org/10.1145/3328923

42. Dev Raj Lamichhane and Janet C. Read. 2017. Investigating Children's Passwords using a Game-based Survey. In *Proceedings of the 2017 Conference on Interaction Design and Children - IDC '17*, 617–622. https://doi.org/10.1145/3078072.3084333

43. Elmer Lastdrager, Inés Carvajal Gallardo, Pieter Hartel, and Marianne Junger. 2017. How Effective is Anti-Phishing Training for Children? In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 229–239. Retrieved from https://www.usenix.org/system/files/conference/soups2017/soups2017-lastdrager.pdf

44. Iolanda Leite and Jill Fain Lehman. 2016. The Robot Who Knew Too Much: Toward Understanding the Privacy/Personalization Trade-Off in Child-Robot Conversation. In

Proceedings of the The 15th International Conference on Interaction Design and Children - IDC '16, 379–387. https://doi.org/10.1145/2930674.2930687

45. Ilaria Liccardi, Monica Bulger, Hal Abelson, Daniel J. Weitzner, and Wendy Mackay. 2014. Can apps play by the COPPA Rules? In *2014 Twelfth Annual International Conference on Privacy, Security and Trust*, 1–9. https://doi.org/10.1109/PST.2014.6890917

46. André de Lima Salgado, Felipe Silva Dias, João Pedro Rodrigues Mattos, Renata Pontin de Mattos Fortes, and Patrick C. K. Hung. 2019. Smart toys and children's privacy: usable privacy policy insights from a card sorting experiment. In *Proceedings of the 37th ACM International Conference on the Design of Communication*, 1–8. https://doi.org/10.1145/3328020.3353951

47. Susanne Lindberg, Pontus Wärnestål, Jens Nygren, and Petra Svedberg. 2014. Designing digital peer support for children: design patterns for social interaction. In *Proceedings of the 2014 conference on Interaction design and children - IDC '14*, 47–56. https://doi.org/10.1145/2593968.2593972

48. Minxing Liu, Haoyu Wang, Yao Guo, and Jason Hong. 2016. Identifying and Analyzing the Privacy of Apps for Kids. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications - HotMobile '16*, 105–110. https://doi.org/10.1145/2873587.2873597

49. Sus Lyckvi and Olof Torgersson. 2018. Privacy and design ethics vs designing for curiosity, communication and children: lessons learned. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services - MobileHCI '18*, 1–8. https://doi.org/10.1145/3229434.3229480

50. Sana Maqsood, Christine Mekhail, and Sonia Chiasson. 2018. A day in the life of jos: a web-based game to increase children's digital literacy. In *Proceedings of the 17th ACM Conference on Interaction Design and Children - IDC '18*, 241–252. https://doi.org/10.1145/3202185.3202753

51. Sumbal Maqsood, Robert Biddle, Sana Maqsood, and Sonia Chiasson. 2018. An exploratory study of children's online password behaviours. In *Proceedings of the 17th ACM Conference on Interaction Design and Children - IDC '18*, 539–544. https://doi.org/10.1145/3202185.3210772

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

53. 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*, 5197–5207. https://doi.org/10.1145/3025453.3025735

54. Sonali R. Mishra, Andrew D. Miller, Shefali Haldar, Maher Khelifi, Jordan Eschler, Rashmi G. Elera, Ari H. Pollack, and Wanda Pratt. 2018. Supporting Collaborative Health Tracking in the Hospital: Patients' Perspectives. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 1–14. https://doi.org/10.1145/3173574.3174224

55. Carol Moser, Tianying Chen, and Sarita Y. Schoenebeck. 2017. Parents' and Children's Preferences about Parents Sharing about Children on Social Media. 5221–5225. https://doi.org/10.1145/3025453.3025587

56. Fnu Nazneen, Fatima A. Boujarwah, Shone Sadler, Amha Mogus, Gregory D. Abowd, and Rosa I. Arriaga. 2010. Understanding the challenges and opportunities for richer descriptions of stereotypical behaviors of children with asd: a concept exploration and validation. In *Proceedings of the 12th international ACM SIGACCESS conference on Computers and accessibility - ASSETS '10*, 67. https://doi.org/10.1145/1878803.1878817

57. Marije Nouwen, Selina Schepers, Karen Mouws, Karin Slegers, Niek Kosten, and Pieter Duysburgh. 2016. Designing an educational music game: What if children were calling the tune? *International Journal of Child-Computer Interaction* 9–10: 20–32. https://doi.org/10.1016/j.ijcci.2016.10.001

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

59. Zachary Pease and Greg Walsh. 2016. COPPA Compliance: A Cooperative Inquiry Perspective. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*, 1453–1458. https://doi.org/10.1145/2851581.2892542

60. Lyta Penna, Andrew Clark, and George Mohay. 2010. A Framework for Improved Adolescent and Child Safety in MMOs. In *2010 International Conference on Advances in Social Networks Analysis and Mining*, 33–40. https://doi.org/10.1109/ASONAM.2010.66

61. Md. Abdur Rahman, Elham Hassanain, Md. Mamunur Rashid, Stuart J. Barnes, and M. Shamim Hossain. 2018. Spatial Blockchain-Based Secure Mass Screening Framework for Children With Dyslexia. *IEEE Access* 6: 61876–61885. https://doi.org/10.1109/ACCESS.2018.2875242

62. Jyri Rajamaki, Paresh Rathod, Anu Ahlgren, Johanna Aho, Mari Takari, and Sami Ahlgren. 2012. Resilience of Cyber-Physical System: A Case Study of Safe School Environment. In *2012 European Intelligence and Security Informatics Conference*, 285–285. https://doi.org/10.1109/EISIC.2012.10

63. Dhanush Kumar Ratakonda, Tyler French, and Jerry Alan Fails. 2019. My Name Is My Password: Understanding Children's Authentication Practices. In *Proceedings of the Interaction Design and Children-IDC '19*, 501–507. https://doi.org/10.1145/3311927.3325327

64. Janet C. Read and Russell Beale. 2009. Under My Pillow: Designing Security for Children's Special Things. In *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology* (BCS-HCI '09), 288–292. Retrieved August 29, 2019 from http://dl.acm.org/citation.cfm?id$=$1671011.1671046

65. 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 - IDC '12*, 200. https://doi.org/10.1145/2307096.2307125

66. Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman. 2018. "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. *Proceedings on Privacy Enhancing*

Technologies 2018, 3: 63–83. https://doi.org/10.1515/popets-2018-0021

67. Jennifer A. Rode. 2009. Digital Parenting: Designing Children's Safety. In *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers*, 244–251.

68. Phakpoom Santisarun and Sirapat Boonkrong. 2015. Social network monitoring application for parents with children under thirteen. In *2015 7th International Conference on Knowledge and Smart Technology (KST)*, 75–80. https://doi.org/10.1109/KST.2015.7051456

69. Cristiana S. Silva, Glívia A.R. Barbosa, Ismael S. Silva, Tatiane S. Silva, Fernando Mourão, and Flávio Coutinho. 2017. Privacy for Children and Teenagers on Social Networks from a Usability Perspective: A Case Study on Facebook. In *Proceedings of the 2017 ACM on Web Science Conference - WebSci '17*, 63–71. https://doi.org/10.1145/3091478.3091479

70. Kiley Sobel, Arpita Bhattacharya, Alexis Hiniker, Jin Ha Lee, Julie A. Kientz, and Jason C. Yip. 2017. It wasn't really about the Pokémon: Parents' Perspectives on a Location-Based Mobile Game. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 1483–1496. https://doi.org/10.1145/3025453.3025761

71.Joshua Streiff, Olivia Kenny, Sanchari Das, Andrew Leeth, and L. Jean Camp. 2018. Poster Abstract: Who's Watching Your Child? Exploring Home Security Risks with Smart Toy Bears. In *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 285–286. https://doi.org/10.1109/IoTDI.2018.00042

72. Saravid A/L Suchaad, Koichiro Mashiko, Nordinah Binti Ismail, and Mohamad Hafizat Zainal Abidin. 2018. Blockchain Use in Home Automation for Children Incentives in Parental Control. In *Proceedings of the 2018 International Conference on Machine Learning and Machine Intelligence - MLMI2018*, 50–53. https://doi.org/10.1145/3278312.3278326

73. Ulia Trifonova and Roman Zharinov. 2012. Concept of the system to protect children's access to information in schools using the DLP-system and RFID-technology. In *2012 12th Conference of Open Innovations Association (FRUCT)*, 1–5. https://doi.org/10.23919/FRUCT.2012.8122098

74. Andreas Tsirtsis, Nicolas Tsapatsoulis, Makis Stamatelatos, Kwstantinos Papadamou, and Michael Sirivianos. 2016. Cyber security risks for minors: A taxonomy and a software architecture. In *2016 11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP)*, 93–99. https://doi.org/10.1109/SMAP.2016.7753391

75. Min-Chun Tuan, Shih-Lun Chen, Ting-Lan Lin, and Ho-Yin Lee. 2016. An efficient micro control unit VLSI design for wearable electronics and sensor networks. In *2016 Pan Pacific Microelectronics Symposium (Pan Pacific)*, 1–7. https://doi.org/10.1109/PanPacific.2016.7428419

76. Asimina Vasalou, Anne-Marie Oostveen, and Adam N. Joinson. 2012. A Case Study of Non-adoption: The Values of Location Tracking in the Family. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work* (CSCW '12), 779–788. https://doi.org/10.1145/2145204.2145321

77. René Vutborg, Jesper Kjeldskov, Jeni Paay, Sonja Pedell, and Frank Vetere. 2011. Supporting young children's communication with adult relatives across time zones. In *Proceedings of the 23rd Australian Computer-Human Interaction Conference on - OzCHI '11*, 291–300. https://doi.org/10.1145/2071536.2071583

78. Greg Wadley, Frank Vetere, Liza Hopkins, Julie Green, and Lars Kulik. 2014. Exploring ambient technology for connecting hospitalised children with school and home. *International Journal of Human-Computer Studies* 72, 8–9: 640–653. https://doi.org/10.1016/j.ijhcs.2014.04.003

79. Chen Wang and Pablo Cesar. 2017. The Play Is a Hit: But How Can You Tell? In *Proceedings of the 2017 ACM SIGCHI Conference on Creativity and Cognition*, 336–347. https://doi.org/10.1145/3059454.3059465

80. Tracy Weru, Joseph Sevilla, John Olukuru, Lorna Mutegi, and Tabitha Mberi. 2017. Cyber-smart children, cyber-safe teenagers: Enhancing internet safety for children. In *2017 IST-Africa Week Conference (IST-Africa)*, 1–8. https://doi.org/10.23919/ISTAFRICA.2017.8102292

81. Marisol Wong-Villacres and Shaowen Bardzell. 2011. Technology-mediated parent-child intimacy: designing for ecuadorian families separated by migration. In *Proceedings of the 2011 annual conference extended abstracts on Human factors in computing systems - CHI EA '11*, 2215. https://doi.org/10.1145/1979742.1979877

82. Svetlana Yarosh, Yee Chieh "Denise" Chew, and Gregory D. Abowd. 2009. Supporting parent–child communication in divorced families. *International Journal of Human-Computer Studies* 67, 2: 192–203. https://doi.org/10.1016/j.ijhcs.2008.09.005

83. Yanfang Ye, Tao Li, and Haiyin Shen. 2015. Soter: Smart Bracelets for Children's Safety. *ACM Transactions on Intelligent Systems and Technology* 6, 4: 1–20. https://doi.org/10.1145/2700483

84. 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*, 1–15. https://doi.org/10.1145/3290605.3300303

85. Hee Jung Yoon, Ho-Kyeong Ra, Can Basaran, Sang Hyuk Son, Taejoon Park, and Jeonggil Ko. 2017. Fuzzy Bin-Based Classification for Detecting Children's Presence with 3D Depth Cameras. *ACM Transactions on Sensor Networks* 13, 3: 1–28. https://doi.org/10.1145/3079764

86. M.S. Zaki, K.H. Alhussein, A.H. Aalquraini, and M.W. Raad. 2018. IoT School Bus: Children Safety. In *Smart Cities Symposium 2018*, 19 (6 pp.)-19 (6 pp.). https://doi.org/10.1049/cp.2018.1387

87. Tab Zhang, Yongle Zhang, Leyi Sun, and Lily Dunk. 2019. HelloBox: Creating Safer and Kid-friendly Communities. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–6. https://doi.org/10.1145/3290607.3309692

88. 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: 10–18. https://doi.org/10.1016/j.ijcci.2017.05.001

89. 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 15th International Conference on Interaction Design and Children* (IDC '16), 388–399. https://doi.org/10.1145/2930674.2930716

90. 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*, 1–13. https://doi.org/10.1145/3290605.3300336