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.

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

ACM Reference Format:

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, such as 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 naïve. 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

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

*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

1While 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 makes.


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.
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
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

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

SELECTIVE PARTICIPATION OF CHILDREN

No children participated in this work.

ACKNOWLEDGMENTS

We thank Rachel Gammons, Nedelina Tchagangalo, 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 Cutholle 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


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.


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.2015.7501456


