‘No Telling Passcodes Out Because They’re Private’: Understanding Children’s Mental Models of Privacy and Security Online

PRIYA KUMAR, University of Maryland, College of Information Studies[1]
SHALMALI MILIND NAIK, University of Maryland, College of Information Studies
UTKARSHA RAMESH DEVKAR, University of Maryland, College of Information Studies
MARSHINI CHETTY, Princeton University, Department of Computer Science
TAMARA L. CLEGG, University of Maryland, College of Information Studies
JESSICA VITAK University of Maryland, College of Information Studies

Children under age 12 increasingly use Internet-connected devices to go online. And while Internet use exposes people to privacy and security risks, few studies examine how these children perceive and address such concerns. To fill this gap, we conducted a qualitative study of 18 U.S. families with children ages 5-11. We found that children recognized certain privacy and security components from the contextual integrity framework, but children ages 5-7 had gaps in their knowledge. Children developed some strategies to manage concerns but largely relied on parents for support. Parents primarily used passive strategies to mediate children’s device use and largely deferred teaching children about these concerns to the future. We argue that helping children develop strong privacy and security practices at a young age will prepare them to manage their privacy and security as adolescents and adults. We offer recommendations to scaffold children’s learning on privacy and security.

CCS Concepts: • **Security and privacy** → Social aspects of security and privacy; • **Social and professional topics** → Children

KEYWORDS

Elementary school-aged children; parents; Internet-connected devices; privacy and security online; contextual integrity; online risks; Internet safety

ACM Reference format:

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. *Proc. of ACM: Human-Computer Interaction: Computer-Supported Cooperative Work and Social Computing,* 1, 1, Article 39 (March 2017), 21 pages.
https://doi.org/0000001.0000001

1 INTRODUCTION

Children increasingly use Internet-connected devices from a young age [21]. As of 2013, 75% of American children under age 9 have access to a smartphone, tablet, or similar device at home, and 7% have their own tablet [9]. Children typically use these devices to watch videos, play games and apps, look for information, complete homework, and socialize, with these activities broadening an fact, children’s online

XX

Corresponding author’s address: P. Kumar, Room 4105 Hornbake Building, South Wing, 4130 Campus Drive, College Park, MD, USA, 20742

DOI: 10.1145/1234

activities rival those of American teenagers, who are "almost constantly" online [25] and for whom mobile devices are so woven into daily life that neither they nor their parents distinguish between online and offline activities [37, 39].

With their increased presence online, children also face privacy and security concerns. These include online tracking and the need to manage private information like passwords. All Internet users face such concerns [38], but most studies on young people have focused on teenagers [3, 25, 53] or children ages 9 and above [28]. This paucity in research with elementary school-aged children is likely due to assumptions that these children do not engage in activities that pose significant privacy and security concerns and that they may not comprehend these complex concepts.

This latter belief is problematic, however, as evidence suggests that children younger than age 9 are capable of understanding complicated concepts. By ages 4-6, most children have developed a "theory of mind," or the recognition that what exists in their mind differs from what exists in the minds of others [40, 51]. Among other things, this enables children to grasp the concept of secrecy, which underpins the ability to manage information [8, 51]. Furthermore, children value privacy because it enables them to engage in identity play, seek advice, form relationships, and immerse themselves in peer communication [26]. Children receive a certain degree of privacy when they engage in these activities offline, and they expect the same online [26]. This aligns with the views of teenagers, who consider "their digital spaces [to be] personal and private" [10, p. 25].

Given that early intervention approaches work best for developing foundational skills, the primary goal of this research is to understand how to help children ages 5-11 manage their privacy and security online. From this work, we can better inform the design of educational resources and interfaces to support children's understanding of privacy and security online. We argue that such resources and interfaces are increasingly critical in a world where use of Internet-connected devices is becoming commonplace in home and at school.

Our study extends related work on how elementary school-aged children perceive privacy and security online in Australia [14] (with children ages 5-8) and Canada [56] (with children ages 7-11 and their parents). We examine a broader age range in the U.S. context, where parenting norms may differ. We also incorporate an additional method, that of hypothetical scenarios [49], as part of our semi-structured interviews.

Three research questions guided this work:

- **RQ1:** What mental models do children ages 5-11 have of privacy and security online?
- **RQ2:** What strategies do children ages 5-11 use to protect their privacy and security online?
- **RQ3:** What strategies do parents use to support their children ages 5-11 in protecting privacy and security online?

To answer these questions, we conducted interviews with 18 families—including 26 children ages 5-11 and 23 parents—in the Washington, D.C. metropolitan area. We used existing theoretical frameworks focused on privacy, childhood development and, in some instances, security, to examine the extent and limitations of children's conceptualizations of privacy and security online. These frameworks helped us to evaluate the strengths and weaknesses of children's understanding of privacy and security online and to identify ways to develop it further.

We offer three main findings. First, children in our study recognized certain privacy and security components, but younger children (ages 5-7) had gaps in their knowledge. This confirms similar findings from existing work [56] and offers novel insights into where children's privacy and security skills can be enhanced. Second, children in our study developed some strategies to manage concerns but largely relied on their parents. This echoes prior work [14] and also offers evidence of different strategies (e.g., lie or hide information) than those previously reported (e.g., leave a website) [14]. Third, parents in our study primarily used passive strategies to mediate children's device use and largely deferred teaching children about these concepts to the future. This extends findings from previous work on parental strategies for managing children's privacy and security online [56] by offering new insights into how parents envision their strategies changing as children grow.

Connecting theories of child development and learning with these three main findings, we recommend ways to help elementary school-aged children grow their existing but limited privacy knowledge. Specifically, we recommend the development of educational resources and interfaces that can help scaffold skill building for children and parents related to privacy and security online.

2 RELATED WORK

2.1 Conceptualizing Privacy

Children tend to define privacy as being alone, managing information, being unbothered, and controlling access to places [54, 56]. While some children also recognize that privacy involves autonomy, this does not define privacy for them [54]. This makes sense because children lack autonomy over much of their life [54]. Furthermore, while scholarship recognizes privacy as a dialectic process [42], children still experience it as "unidirectional or one-sided" [54, p. 214].

While adults have a greater say in the role privacy plays in their life, the concept itself remains difficult to define. Nissenbaum posits privacy as "neither a right to secrecy nor a right to control, but a right to *appropriate* flow of personal information" [36, p. 127, emphasis in original]. Since the Internet facilitates unexpected information flows, many online activities raise privacy concerns [38]. For example, disclosing a fact in an email creates a record that persists long beyond face-to-face interactions. Nissenbaum's contextual integrity framework [36] is particularly well suited for evaluating how people conceptualize privacy online because it explores how people expect information to flow in a given context [1]. By identifying discrete components that contribute to a person's privacy expectations, this framework enables us to examine children's understanding of privacy at different levels of nuance or complexity.

The contextual integrity framework states that information flows according to the *norms* that govern a given situation. These norms vary based on the context of the situation and are shaped by cultural, ethical, moral, or legal factors [36]. The framework includes four components:

- ***Context:*** The backdrop of a given situation that informs what norms govern the information disclosure. For example, a child might feel comfortable disclosing that she played a game on a tablet at home but hesitate to disclose that she played a game on a tablet while at school. In other words, the home context facilitates leisure activities more readily than the school context.
- ***Attributes:*** The types of information at play. For example, a home address is far more sensitive than a person's favorite flavor of ice cream.[2]
- ***Actors:*** The parties involved in the information disclosure. This includes the subject of the information (who it is about), the sender of the information, and the recipient of the information. For example, a teacher (sender) may disclose information about a student (subject) to the student's parent (recipient).
- ***Transmission Principles:*** The way information is transmitted from sender to receiver. For instance, disclosing information in an email could raise more privacy concerns than disclosing the same information in a face-to-face conversation because of the persistence of an email record.

We extend the growing body of work on the contextual integrity framework [1, 36, 38] by showing how it can also help us understand the way children, not just adults, conceptualize privacy online.

Privacy and security are related, but distinct, concepts. Information security involves three main goals: Maintaining the integrity of personal information that is stored and transmitted through networks; authenticating users who access personal information; and preserving the confidentiality of personal information [46]. For children, security means that data they store or transmit online is not compromised, that accounts with their information are restricted to approved users, and that information they share in

[2] Which should always be chocolate.

one context is not automatically shared in another context (i.e., a message sent to a friend is not automatically sent to a parent). We use this framing to understand how children ages 5-11 conceptualize security online.

2.2 Child Development, Mental Models, and Scaffolding

To help children navigate privacy and security online, we first need to understand how they conceptualize these ideas. A mental model is the way a person thinks something works; people use mental models to judge the likelihood of something occurring, to make decisions, and to understand other people's actions [24]. Prior work has used the mental models approach to understand how people think about privacy and security [6, 49, 55]. McReynolds et al. [33] used a mental models approach to understand how children ages 6-10 conceptualized privacy threats for Internet-connected toys. In this study, we focus on children's mental models when using more general-purpose devices, since toys are only one part of the ecosystem of Internet-enabled devices that children interact with on a daily basis.

We specifically aim to understand children's privacy and security mental models so that we can more effectively support their development. We draw on Vygotsky's zone of proximal development (ZPD) theory [48] to guide our understanding of how we can advance children's mental models of privacy and security. An individual's ZPD is the distance between what he or she can do without help and what he or she is capable of doing with help. Learning occurs as a child engages in the hardest tasks he or she can do (with help) until the help is no longer needed. The assistance provided in that space, called scaffolding, helps the learner develop to the point where he or she no longer needs support [48, 50]. We use Nissenbaum's contextual integrity framework [36] to understand children's mental models with respect to privacy and security. This helps us identify the types of scaffolding parents can provide their children within their ZPD. We then consider ways to better support children and parents in their ZPD interactions in face-to-face and software-realized scaffolding [43] contexts.

2.3 Children and Privacy and Security Online

Prior work has identified privacy- and security-specific risks that children face online. Experts warn that children and teenagers put their privacy at risk by disclosing information inappropriately or sharing information on social media that reflects poorly on them [37]. Additional privacy implications stem from the mining of children's data for marketing purposes, the role of online activities in identity play and relationship building, and the normalization of surveillance [35, 44, 47]. Security concerns for children focus on physical and mental safety, such as preventing exposure to inappropriate content and stranger danger, or the risk that children will encounter and interact with strangers online who may be sexual predators [14, 56]. Advances in the Internet of Things also expose children to risks. For instance, adversaries could hack into Internet-connected toys and access data about a child or interact directly with a child who uses the toy [33].

Extensive research documents how teenagers and children over age 9 experience and manage risk online [3, 25, 28, 37, 53]. These studies report that teenagers are vulnerable to such threats as cyberbullying or online harassment, receiving sexual solicitations, viewing explicit content, or receiving contact from a stranger [27, 31, 53]. Studies of European children ages 9-11 suggest that this younger demographic experiences less risk online than teenagers, since children in this age group may not use social media or spend as much time online as teenagers [29]. However, this is changing as use of Internet-connected devices among children under age 9 gains prevalence [9, 21].

As described in the Introduction, two studies explore how children under age 9 conceptualize risk online. Through focus groups in Australia, Ey and Cupit [14] found that while children ages 5-8 could identify several categories of risks, a sizable number could not identify certain online activities as risky. Our study extends this work by using the contextual integrity framework [36] to unpack why children perceive that an online activity implicates (or does not implicate) privacy and security. Through interviews with parents and children ages 7-11 in Canada, Zhang-Kennedy et al. [56], found that children perceive threats from peers, 'bad' media, 'mean' strangers, and parents, while parents perceive threats from media,

technology, strangers, peers, and children themselves. Our study builds on this work by showing how children evaluate potentially risky situations online and decide how to handle them.

2.4 Parental Mediation of Children's Online Risk

Parents recognize that their role as mediators of their children's technology use begins shortly after their children are born [20]. Parents use a variety of strategies to mediate online risk exposure for children ages 7 and above. These include talking to their children, being around or next to them when they go online, setting rules for device use, helping them set up accounts online, and using software to monitor their children's online activities [12, 30, 56]. Wisniewski et al. [52] distill parent strategies for teenagers into two forms of mediation: direct parental intervention (e.g., using parental controls, setting up children's accounts) and active parental mediation (e.g., talking with children, reviewing what they share online). They find that a combination of the two approaches may best help parents mitigate teenagers' exposure to risk while also enabling teenagers to take advantage of online opportunities [52].

Despite the variety of strategies parents use to mediate teenagers' exposure to risk, parents may still underestimate the extent to which their teenagers experience risk online [53]. It is unclear whether the same holds for children under age 13. However, previous work has demonstrated that parents and children share different views on technology use and different interpretations of family communication about the topic [2, 10]. In essence, managing technology use within the family remains an evolving, dynamic, and situated endeavor [19, 32]. We build on this work by exploring how parents consider privacy and security concerns for children under age 12 and providing further evidence of parental mediation strategies.

3 METHODS

In December 2016 and January 2017, we conducted face-to-face semi-structured interviews with 18 families (23 parents and 26 children ages 5 to 11) in the Washington, D.C. metropolitan area. We also walked through a series of hypothetical scenarios with children, a technique previously used to explore people's understanding of security [49]. We sent recruitment information to local parenting listservs. While we used the terms "privacy" and "safety" in the title of the project, we framed it as an exploration of how children and parents think about the benefits and risks of going online.

Each family received a US$30 Amazon gift card for participation. Before the interviews, we asked parents to fill out an online survey that included questions about their demographics and their child's technology use. We also included two behavioral scales: one focused on general caution and technical protection [4] and the Security Behavior Intention Scale (SeBIS) [13]. These scales offered a standardized format to gauge how privacy- and security-conscious the parents in our study were. The University of Maryland's Institutional Review Board (IRB) approved this study.

3.1 Participant Demographics and Children's Device Use

We interviewed 23 parents –16 mothers and seven fathers (median age: 39 years; age range: 32-53). We also interviewed 26 children –14 girls and 12 boys (median age: 8 years, age range: 5-11). We received demographic information from 20 parents; 14 self-identified as White, three as Latino, and one each as African-American, Asian, and other. Parents in our study were highly educated: five held bachelor's degrees and 15 had at least some graduate education. Children from 16 families lived with two parents; children from two families lived primarily with their mother but periodically saw their father.

Table 1 provides basic information about participating families and the devices children used at home. In terms of general privacy and security awareness and behaviors, the 20 parents who filled out the survey had a median score of 3 on the general caution scale and a median score of 3.5 on the technical protection scale, suggesting they are about average or slightly above average on privacy-related behaviors. They had a median score of 3.6 on the SeBIS scale, suggesting they are slightly above average on security-related behaviors.

Table 1. Basic Information about Participating Families and Devices Children Use at Home

Family	Parent Participants	Child Participants, Age	Devices Children Used at Home
A	Mother	Boy, 8; Girl, 8	Own iPads, XBox
B	Mother, Father	Boy, 11*; Boy, 8	iPads, iPhones, iPods, Chromebook
C	Mother	Boy, 9; Boy, 7; Girl, 6; Girl, 6	Family desktop, iPads, mother's iPhone
D	Mother, Father	Girl, 7	Kindle, mother's iPad, mother's iPhone, mother's old laptop,
F	Mother, Father	Girl, 7	iPad, mother's "computer" (Surface tablet with keyboard), Amazon Echo
G	Mother	Girl, 8	Kindle, family laptop connected to large monitor
H	Mother	Boy, 8	At mother's house: Samsung Galaxy X2 smartphone (on WiFi), mother's iPad, mother's smartphone, laptop At father's house: PlayStation
I	Mother	Boy, 10	Own iPad, mother's smartphone, family computer
J	Mother	Girl, 11*; Boy, 7	iPhone, iPads
K	Mother	Girl, 6	Kindle Fire, mother's smartphone, family computer
N	Mother, Father	Boy, 6	Mother's smartphone, own laptop, Amazon Echo
P	Mother	Boy, 8; Boy, 6	Kindle, mother's smartphone, family computer
Q	Mother	Girl, 7	At mother's house: mother's smartphone, mother's iPad, laptop. At father's house: father's smartphone, father's iPad, own tablet
S	Mother	Boy, 5	iPad
V	Father	Girl, 11*; Girl, 8*	Own Samsung smartphones, family laptop
W	Mother	Boy, 10	iPad, Kindle Fire, own Kindle eReader
X	Mother, Father	Boy, 6	Mother's laptop, iPad, parents' iPhones, Nintendo Wii
Y	Father	Girl, 10	iPad

* Child has own smartphone

3.2 Interview Procedure

Interviews lasted one to two hours; most were around 90 minutes. At least one parent and one child from each family participated, and we welcomed participation from additional family members. Interviews occurred in participants' home or at a public venue such as a library. After obtaining parental consent and child assent, we interviewed the child and then the parent. Parents remained in the room or went to a nearby room during the child interview, depending on the public or private nature of the venue and comfort level of the family. Most children left the room or did other activities during the parent interview.

While we acknowledge that the presence of parents and children nearby may have influenced participant responses, we also sought to ensure that our participants felt comfortable with the interview setup, given the young ages of children we interviewed. We also endeavored to minimize the methodological challenges associated with interviewing children. These include the interviewer's need to

build rapport despite essentially being a stranger to the child, the need to gain trust from parents, and the need to host the interview in a location that is comfortable for the child and the parent [23].

The semi-structured child interview began with questions about what devices children used and what activities they liked to do on those devices. We asked what their parents did or did not allow them do on the devices, how they found content such as videos or games, and the general types of experiences they had on the devices. We also asked children about their technology use in school, including questions about devices, activities, rules, and experiences.

We did not ask children about risk directly, but instead we asked about specific types of experiences that literature suggests can involve risk (e.g., something that scared them, something they did not understand, something that may have been inappropriate, something mean) [53, 56]. If children mentioned privacy, security, or related concepts such as secrets, we asked children to describe what those words meant or to provide examples of them. While we collected data on a range of topics, this paper focuses on findings related to privacy and security. In-depth discussion of broader risks and harms, for example viewing inappropriate content or cyberbullying, as well as device use in school, remain out of scope for this paper. We intend to analyze those results in future work.

After the semi-structured interview with children, we moved to the "hypothetical scenario" portion of the interview [49], which we framed as a game. We told children to imagine they had a new friend who just received a new tablet. We then placed six index cards facedown. Each card included a scenario involving the device and a question asking what the child believed the friend would do in response (*i.e., Someone our friend doesn't know just sent our friend a message on the tablet. What does the message say? What does our friend do?*)

These scenarios were based on threats identified in Zhang-Kennedy et al.'s study [56]: siblings looking at a device; parents looking at a device; receiving a message from an unknown person; a friend asking for a password; determining whether content is appropriate; and encountering something scary. This helped us better understand how child participants thought about privacy and security risks even if they had not experienced them (or did not remember doing so).

Two children drew something in response to one of the prompts, and all children verbally explained their responses. For two families, the semi-structured interview with children lasted an hour and covered most of the hypothetical scenarios, so we did not play the game.

After the child interview, we conducted a semi-structured interview with parents. We asked how long their children had used the devices, how parents decided what, if any, parameters to set for their children related to the devices, what strategies they used to mitigate or manage risk, what (if any) challenges they faced, and how they saw their approach to technology evolving in the future. We also followed up on information their children told us and invited parents to add to or correct that information.

All interviews were audio-recorded. The first and second authors conducted eight interviews together. The first author conducted the remaining 10 interviews alone.

3.3 Data Analysis

We transcribed the interviews and used an inductive approach to develop codes and categories [45]. The first author reviewed a subset of the interviews and developed an initial codebook, which the team discussed. Two researchers coded each transcript: the first author coded all transcripts, and the second and third authors collectively coded all transcripts. While coding, we discussed codes that were unclear and iteratively revised the codebook. In cases of disagreement, we discussed the codes and relevant text until we reached consensus.

We created codes related to activities children did on devices (e.g., *play-games*, *watch-videos*), constraints that parents set on those activities (e.g., *activity-not-allowed*), challenges children faced (e.g., *disclose-personal-information, manage-passwords*) and strategies children and parents used to address concerns (e.g., *consult-parents, use-parental-controls*). We then created categories of similar codes and examined each category for evidence of children's understanding of privacy as reflected by contextual

integrity components such as *context, attributes, actors,* and *transmission principles*. Drawing on these categories and relevant literature, we organize our findings around several key themes.

4 FINDINGS

We present our findings in five sections. First, we describe how children and some parents in our study found the idea of being online difficult to define. Second, we demonstrate how the contextual integrity framework explains the way children in our study conceptualized privacy and security concerns. Third, we review what strategies children used to address these concerns. Fourth, we identify parents' strategies to mediate their children's technology use. Finally, we show how parents largely defer addressing risks to the future, when their children will be older.

4.1 "Being Online" is Difficult to Define

Much like teenagers [39], children and parents in our study had a blurred distinction of online and offline behaviors. This affected their perspectives on privacy and security. As shown in Table 1, children in our study used tablets, smartphones, and computers. Echoing prior work in the U.S., U.K, and Canada [9, 21, 56], children said that they overwhelmingly used the devices to play games and watch videos. Children in our study also searched for general information out of personal curiosity or to support their homework. A few mentioned using Internet-connected devices for other activities such as reading, playing music, or looking at photos. Although all children in our study were below age 13, the minimum age to use most social media sites, three currently used social media and two others had done so in the past. All children except one, a kindergartener, said they used a computer or a Chromebook in school. There, they used the devices for similar activities as at home: they played math and reading games, watched videos, went to websites their teachers told them to view, wrote collaborative documents, and managed schoolwork.

The devices that children used were capable of connecting to the Internet and bringing their users online—allowing them to access websites, messaging functions, email, or other applications. However, many children in our study struggled to define what being online meant. They often equated being online with seeing other people or players in a game.

Parents from five families maintained narrower definitions of being online, which focused primarily on going to specific websites or looking for information. Parents from Family A and Family S said that their children did not "*go online*" or "*surf the web*," although their children often used iPads. While a 6-year-old boy from Family N often used his parents' smartphones, his parents said he "*very rarely*" went online; he did so only to look up information such as a song or movie. This suggests that at least a subset of parents in our study saw going online as accessing websites on a computer or looking up information on the Web, and that they did not consider playing games on a tablet or watching videos on mobile apps to be online activities.

One explanation for this difficulty is that children use an increasing number of Internet-connected devices, such as iPads, smartphones, smart TVs, and smart assistants. This makes it hard to track when children ages 5-11 are on the Internet, a finding that holds for teenagers as well [39]. This suggests that it is becoming more challenging to help parents and children navigate privacy and security online, since the boundaries of being online are changing rapidly as use of Internet-connected devices becomes a ubiquitous part of family life.

4.2 Children Apply Contextual Integrity to Privacy and Security Threats from Inside/Outside Home

Zhang-Kennedy et al. suggested that while Canadian children age 7-11 accurately perceive privacy and security risks, they "do not yet know how to apply the concept of privacy online" [56, p. 397]. Extending these findings to the U.S. context, we found that children in our study demonstrated a reasonable but limited understanding of privacy online. For instance, they demonstrated at least some understanding of components of the contextual integrity framework:

- *Attributes:* Children in our study identified certain types of information as sensitive.

- *Actors*: Children felt comfortable sharing information with certain people and not others.
- *Transmission Principles:* Children ages 10 and above understood that sharing information online could introduce different types of privacy concerns. With the exception of one eight-year-old girl, children ages 5-9 did not demonstrate this kind of understanding.
- *Context:* Children showed evidence of using contextual norms to evaluate whether to disclose information online.

That said, children in our study understandably faced challenges in maintaining privacy and security online, and they sometimes failed to recognize privacy or security concerns. For example, more than a quarter of children revealed a password during the interview, and a few said there were circumstances in which they would reveal their address in a message online. These challenges highlight where interventions can help children better understand privacy and security online.

4.2.1 Attributes: Types of Sensitive Information

Children in our study identified several types of information as sensitive, including name, age, address, username, password, lists of birthday presents or candy eaten, YouTube videos watched, points on ClassDojo (a classroom management app), notes to other children, notes about what someone did today, secrets, "*family business*," and "*stuff that you don't want people to know*" (Family G girl, age 8).

Many children in our study associated privacy and security online with rules about information disclosure. For example, a 6-year-old girl from Family C said, *"No telling passcodes out because they're private.*" Siblings from Family A described safety on an iPad as "*not telling anybody about…your personal information*" (Family A boy, age 8) or "*your password*" (Family A girl, age 8). This suggests that children ages 5-11 largely rely on explicit rules, rather than internalized *norms*, to determine when information can be disclosed online.

4.2.2 Actors: How Trusted Others Shape Privacy and Security

Children in our study felt comfortable sharing information with a parent, and in some situations, with people outside the family. Most children understood that they should not share information with unknown people online. But two said they would in the context of arranging a play date.

Many younger children in our study (ages 5-7) saw no issue with a parent looking over a child's shoulder while the child used a device. However, several children in our study said a child in this situation would feel "*scared*" because that child might be doing something the parent does not allow. This finding extends that of Zhang-Kennedy et al. [56] by suggesting that children under age 7 also recognize that parents can pose a privacy threat to children. But this recognition was less pronounced in our study, as our child participants were more concerned about getting in trouble than perceiving parents as a privacy threat.

Two children in our study said that a child might try and prevent parents from looking at a device while a child uses it, but none questioned the parent's authority to monitor children in this manner. A 10-year-old boy from Family I said parents could look at the device "*because the parents are the ones who bought that for them.*" He added that children would get "*a bad feeling*" if their parents watched them without telling them.

Overall, children in our study perceived that parents have a right to monitor their online activities. An 11-year-old girl from Family J recognized that even though a child's right to privacy increases in middle school and high school, "*the parents have the right to know what's going on.*" Only one child in our study said her privacy interests outweighed her mother's right to know. She said she would not share a password with her mother due to the types of information she kept on her device:

> "Because I don't want my mom getting on my iPad and seeing what her future birthday presents [are]. And all my private stuff….[like] food and candy…[and] when we're [friends] going to have secret play date" (Family D girl, age 7).

In some situations, children in our study felt comfortable sharing passwords with other people they knew. A 7-year-old girl from Family F shared a device password with a neighbor, who was also a family friend. An 8-year-old boy from Family H and an 11-year-old boy from Family B shared passwords with

friends; the Family B mother knew about this practice and raised no concerns about it. A 6-year-old girl from Family C shared a school password with a classmate who lacked her own account; the girl said her teacher suggested this workaround.

Most children in our study recognized they should not share sensitive information such as a password or address with an unknown person. When asked how a child should respond if they receive an online message asking for their address, most said the child should tell a parent or refuse to disclose the information. However, two suggested the child could share the address if it were for a play date, not recognizing that this could lead to a physical safety concern.

Overall, this suggests that children largely understand how to make disclosure decisions that involve a known actor, like a parent or neighbor, but that they may struggle when considering an unknown actor, like someone sending a message online.

4.2.3 Transmission Principles: How Sharing Information Online Implicates Privacy

A few children in our study recognized that the medium of the Web affects the visibility of information. An 8-year-old girl from Family G described a "*privacy warning*" she saw on YouTube:

> "It says, 'privacy warning,' that, um, like, people will be, like, YouTube will be watching what you're watching on YouTube. Like, they're seeing everything you're gonna watch (Family G girl, age 8).

A 10-year-old girl from Family Y said "*it's not, like, fully possible to have complete privacy*" online because websites such as YouTube and Musical.ly can still see what users do on the site. She acknowledged that some sites allow users to control this visibility:

> "[I]t depends on what you share on but on YouTube, yes [information is public]. On Instagram or something else, it's only people who follow you and people that you follow and stuff. You can choose to share them with those certain people" (Family Y girl, age 10).

In contrast, another child viewed Instagram as a more open site compared to Snapchat.

> "I have Snapchat, but it's more of a closed social media, so you can only chat with your friends. So it's not as ... open as Instagram, Facebook or Twitter" (Family J girl, age 11).

One child explicitly acknowledged that the way information flows can affect privacy. A 10-year-old boy from Family I said that a child should not reveal an address if someone online sends a message requesting it. Even if the message comes from a friend:

> "They could just talk in person....I just think he should do it around the parent and tell his friend." [If someone shares their address online,] "other people could get it....it can be like blogged by someone and then someone else can get it" (Family I boy, age 10).

This child recognized that talking in person conveys information without leaving a clear trace. Sharing it online, however, makes it easier for the information to spread beyond its intended recipient. It is not that the address should never be shared, but rather, it should be shared in a way that reduces risk to privacy and security. This child made a connection between the medium of communication and the potential risk of spreading sensitive information; no other children in our study demonstrated such a clear understanding of *transmission principles*. This suggests that children under age 10 still have a limited understanding of how the medium through which information is transmitted affects the privacy and security implications of sharing that information.

4.2.4 Context: Using Contextual Norms to Make Decisions

Contextual integrity argues that people do not seek complete control over information about themselves. Rather, they want information to be shared appropriately, that is, shared in a way that fits the *context* of a given situation [36]. Children in our study often used the heuristic of, could this cause trouble to determine whether to disclose information. A 6-year-old boy from Family X would not talk to people online, "*because it might get me into some trouble.*" Many children in our study also understood why disclosing personal information online could pose a risk. For example, revealing a password could enable unauthorized access, by letting a "*bad person...look onto [a child's] personal accounts*" (Family Q girl, age 7).

> "[I]f someone may get my password, maybe they would use it for something that I didn't do, and I might get in trouble for something I didn't do. And I don't wanna risk getting in trouble for something I didn't do if I didn't do it" (Family G girl, age 8).

> "Because if it was a bad person you would not know and...they might call the police on you...And they would blame you, but you really did not do anything wrong...That's why you should not tell them your phone number or your passcode" (Family C girl, age 6).

Children in our study also said disclosing information like an address online could raise safety concerns related to burglary or kidnapping. One child mentioned the risk of identity theft.

> "Where [a child] lives is personal information...and they can't just share it to anyone who they don't even know, because it could lead to identity theft, and their identity could be stolen because [the person asking for information] know[s] personal information about them. If they keep on saying personal information, [the person] could really get enough information to pretend to be them, and ruin their future" (Family J girl, age 11).

A few children in our study mentioned that someone who accessed their devices could "*mess up*" or "*delete*" their games, compromising the integrity of their information. Sharing a password could also facilitate impersonation.

> "Well, if they're a stranger, like, maybe they could post something bad to our friends and then our friends wouldn't like us anymore just because of them" (Family P boy, age 8).

Children in our study showed basic knowledge of the security goals of authentication and integrity [46]. They recognized that passwords serve as access controls, and a few understood that giving another person access to their games could compromise the integrity of their game data. But when discussing the contexts in which disclosing information online was or was not appropriate, children used fear of punishment as a deciding factor more than concern over threats to privacy and security. This highlights the need for children to understand why they should act in ways that protect their privacy and security. If children understand why certain rules for Internet activities exist, they will be better equipped to manage privacy and security in situations when parents are not physically present or no longer set or enforce these rules for them.

4.2.5 Children's Challenges in Understanding Privacy Contexts

Children in our study did not always demonstrate good judgment related to privacy and security online. From a contextual integrity perspective, children sometimes struggled to understand what norms apply to different contexts. This was clear when it came to passwords. Adults generally know when it is appropriate to share a password; some children ages 8 and under in our study did not. A 6-year-old girl from Family K asked the interviewer, "*Do you want to know my password?*", and seven children disclosed at least part of a password during the interview.

One child explained why her actions were not a risk:

> "Well, you don't have, like, Chromebooks like we do….There's no privacy in Chromebooks….you don't really get to any of our private information by a Chromebook" (Family G girl, age 8).

For this child, the interviewer's inability to access her school-owned Chromebook as well as the lack of "*private information*" on the device mitigated the risk of her revealing the password. These contextual factors made her feel she did not need to follow the rule about not sharing passwords. Other children in our study who revealed passwords did not appear to realize their actions or did not explain why they had done so. These examples show where scaffolding from a trusted adult about how rules can change in different contexts can help a child develop practices that protect their privacy and security across various situations.

Two children mentioned the idea of a strong password, but most did not seem to realize the weakness of certain passwords. An 8-year-old girl from Family G said her religious-school teacher set the girl's online school account password to be the girl's name. Three children said their passwords involved their birthdays. A 10-year-old boy from Family I said his school used children's birthdays as their school

account passwords. He said people have guessed other students' passwords and gotten into their accounts, but this has not happened to him "*because I didn't tell anyone my birthday.*" An 8-year-old boy from Family H appeared to realize the weakness of this password, but it did not seem to bother him.

> "[M]y phone password is my birthday. Year that I was born. And my mom knows that, she's the only one that knows that. Since I just mentioned it right now, everyone [in the house] might know it because they all know when I was born" (Family H boy, age 8).

An 8-year-old girl from Family G said her mother makes her passwords, writes them down, and puts them in a box. When the girl needs to log in to an account, she checks the box rather than having to remember the password. Most other children said their teachers keep the passwords for the children's school accounts on index cards, which they hand out when children have to log into a computer. Two children said their parents had to reset their iPads because the children forgot the passwords.

Children are understandably forgetful, something adults should factor into their mediation strategies. However, some of their techniques (i.e., using weak passwords) represent poor security practices [56], which can complicate adults' efforts to foster good habits in children. In other words, this finding shows that children ages 5-11 are heavily influenced by the privacy and security practices of trusted adults, whether or not those practices are the best ones for protecting privacy and security online.

4.3 Children Rely on Parents, Lie, or Hide Information to Protect Privacy and Security

Most children in our study said they would talk to their parents if they encountered something unknown while online. This is more specific than the sources of advice for teenagers [52], who consult friends, peers, siblings, parents, teachers, and online resources, and for children ages 5-8 [14], who consult adults. A few children in our study mentioned additional strategies, such as providing false information or trying to hide information from prying eyes. These strategies are more nuanced than simply closing a website, which children ages 5-8 report doing [14], but they are not as sophisticated as strategies that teenagers use [52], such as deleting content, blocking users, or deactivating accounts.

4.3.1 Child Strategy 1: Consult Parents

Most children in our study saw parents as a resource to help them manage privacy and security online. An 11-year-old boy from Family B said that a few years ago, "*scammers*" on Instagram followed his public Instagram and left comments saying that if he gave them his XBox password, they would give him "*coins and stuff*" to use in online soccer games. He asked his mother for the password, and she told him it was a scam. She then changed his Instagram settings so his profile was private.

No other children in our study reported an experience where someone online asked them for a password. If this happened, they said they would tell their parents or not provide the information. Some said they would check if the person asking for information provided a name or picture. This underscores the important role that parents play in shaping children's understanding of privacy and security online.

4.3.2 Child Strategy 2: Provide False Information

A few children in our study recognized the strategy of providing false information as a way to protect privacy and security: an 8-year-old boy from Family H suggested providing a false password if asked; three children ages 7, 7, and 9 suggested providing a false address if asked; and an 8-year-old boy from Family A suggested not using a real name as a username in Minecraft. The other children in our study did not use this technique.

4.3.3 Child Strategy 3: Restrict Access to Information

Two children described strategies for deterring friends or siblings from seeing their information on a device. A 10-year-old girl from Family Y added a password to her iPad because she did not want friends to see, for example, what YouTube videos she watched, in case they would make fun of her viewing selections. An 8-year-old boy from Family B did not want his younger siblings to play his game apps.

When he shared his iPad with them, he moved the apps into a section called "*Private Games*". However, this was not very effective since his younger siblings could not read.

These two children understood, on a basic level, the importance of security goals such as authenticating users and preserving the integrity and confidentiality of information [46]. Some children in our study recognized they could act in ways that support their privacy and security. However, most children still relied heavily on their parents to understand how to address privacy and security online. As children grow, they will need to develop their own understanding of these concepts so they can create strategies to manage their own privacy and security. Furthermore, if the practices they learn at a young age do not adequately protect their privacy and security, they will face the task of "unlearning" poor privacy and security habits and learning better ones.

4.4 Parents Use Passive Measures to Monitor Children's Device Use and Protect their Privacy and Security

Parents in our study used many of the strategies outlined in prior work to mitigate their children's privacy and security risks [12, 31, 56]. Most set some type of boundary for acceptable behavior on the devices. They enacted these guidelines by maintaining ambient awareness while their children used devices and by using some type of parental control. A small number of parents checked their children's devices. Prior work defines these as active mediation strategies [13, 53], however, parents in our study used these techniques in fairly passive ways. Parents did not believe their children were currently exposed to many privacy or security concerns, thus they did not see these strategies as active ways to mediate children's risk online.

4.4.1 Parent Strategy 1: Set Boundaries

Most parents in our study set general boundaries about what their children could do on their devices. Naturally, specifics varied across families. For example, parents from five families felt their children should not use YouTube, while others allowed their children to use the video-sharing app. Some parents created separate user accounts on Netflix for their children or let their children use YouTube Kids, since these sources curated content specifically for children. Parents also wanted children to check with them before playing or watching something new. This helped parents remain aware of how their children used their devices.

> "They [children] know how to get to Safari, it pops up to Google, you can type something in….They can type it in with somebody standing there. In the periphery, there's somebody there who, or they [will say], "I want to try this game." I'm like, "Okay, let me see what it is. You can figure out, but show me how to get there. I want to see what this is before you fully embark and go and do this" (Family C mother).

However, as Mazmanian and Lannette [32] explain, enacting guidelines around children's technology is not straightforward. For example, a father from Family V said his daughters needed permission before they could use new apps, but one daughter mentioned downloading other social media apps and games without seeking permission. Other children in our study referenced the flexibility of their parents' guidelines, for example, saying their parents did not always strictly enforce time limits on device use. This is not to suggest that rules are ineffective, but rather to underscore that managing children's technology use, like other everyday activities, is a complex, contextual, and dialectic process [32]. There is no one-size-fits all approach to teach children about privacy and security online; rather, it needs to be woven into children's everyday experiences of online activities.

4.4.2 Parent Strategy 2: Maintain Ambient Awareness

In ten families, children typically used devices in a common area or when parents were around. This enabled parents to maintain a general awareness of what their children were doing. Listening for game or video sounds from the device gave parents in our study a sense of what their child was doing without needing to look. Some were more lax, while others were a bit more active, as this mother:

> "I always kind of nose over his shoulder. I do that a lot. Sometimes I try to sneak up so he doesn't really realize I'm coming to look. I do that to see what he's doing, but...I can also kind of tell. I can listen, and if it's too quiet, what are you doing. But most of the time, if I can hear the sound, like Minecraft, you can hear those zombies the whole time. Crunch, crunch, crunch. Oh, I know he's still on Minecraft" (Family H mother).

Parents in our study maintained awareness of their children's online activities. This puts them in a good position to proactively and periodically mention ideas related to privacy and security online in conversations with children. This would be a fairly simple way to integrate such concepts into children's everyday experiences.

4.4.3 Parent Strategy 3: Use Built-In Parental Controls

Parents from seven families mentioned using some type of parental control on a device. These controls restricted inappropriate content or set time limits for device use, and did not relate directly to privacy or security concerns. None of the parents in our study said they currently used additional blocking, filtering, or monitoring software on devices that children used.

4.4.4 Parent Strategy 4: Monitor Children's Devices

Parents from three families checked the devices their children used, though only one said she did so regularly. A mother from Family B checked her 11-year-old son's smartphone every one or two evenings. When he used Instagram, she also reviewed his activity there; the boy was aware of his mother's practices. She saw this as part of her responsibility, and told him when he received the phone:

> "I want to be able to check what's going on until you get to a certain age. And, you know, it's not that I'm disrespecting your privacy, but it's, it's my job to look out for you as a parent" (Family B mother).

Parents from two families had checked the browsing history on the devices their children used, but they did not do so regularly. One parent saw sexually suggestive sites in the history, and he discussed this with his daughter.

In sum, parents in our study were not simply handing their children devices without any guidance. They recognized their responsibility to mediate their children's technology use, but they did not see these efforts as focused specifically on protecting children's privacy and security.

4.5 Parents Are Aware of Risks But See Privacy and Security as *Future* Concerns

Overall, parents' primary concerns about their children's device use focused on screen time, stranger danger, and cyberbullying. From a privacy perspective, some were concerned about children's self-presentation online. Security-wise, parents took steps to protect themselves from children's actions (e.g., children buying apps or accessing parents' information). But most parents in our study believed that their children did not currently face many privacy or security risks. They deferred addressing such concerns to the future, despite the fact that experts warn parents against this type of complacency [31].

4.5.1 Concerns About Children's Self-Presentation Online

The only privacy-specific concern that parents in our study described focused on children's self-presentation online. However, only three children in our study (an 8-year-old girl and two 11-year-old girls) currently used social media (Musical.ly and Snapchat). Two other children (boys ages 8 and 11) had used Snapchat and Instagram, respectively, in the past.

Echoing expert warnings [37], parents from Family B and Family I expressed a general desire for children to recognize that when they share information online, others form judgments based on those disclosures. Parents from Family F and Family V related this concern to their own children. A 7-year-old girl from Family F knew how to take pictures using a smartphone, but she did not upload or share them. Her parents' only concern about her device use was that she would record a video of herself doing

something mundane, share it online, and the video would go viral. They feared she would be embarrassed by the attention, but they did not see this as a privacy or safety concern.

> "Yeah, I don't think it's dangerous, like, dangerous as someone could see something and come here and, I don't know, like, not privacy level, like, where someone bad could do something. But, eh, yes, in the sense of like people watching her doing something weird or something odd, or, or embarrassing" (Family F father).

A father from Family V similarly expressed concern that his daughters, ages 8 and 11, would share pictures or videos on the social network site Musical.ly that inadvertently exposed their chest. Law enforcement officials have raised similar concerns that child predators are using the site to ask children to send inappropriate pictures [34].

Some parents in our study saw self-presentation as a concern, but they could not clearly articulate why. Helping parents link their concern about a given online activity to the consequences that a child may experience could help parents scaffold their children's efforts toward practices that protect their privacy and security.

4.5.2 Concerns About Children Downloading or Accessing Content

Nearly all parents in our study wanted to retain control over what apps were on a device. To do so, they did not share the password for the device's app store with children. Many said their children had to seek their permission before getting a new app on the device. Two parents also said they withheld the app store password to minimize the chances that their children would spend money or reveal the password to someone else. A mother in Family F had to change a password after her 7-year-old daughter made in-app purchases. As described earlier, an 11-year-old in Family B received requests for an Xbox password on Instagram; he and his mother both said he would have revealed the password had he known it. Parents are wise to guard passwords connected to payment methods; Amazon is refunding US$70 million to parents whose children inadvertently made in-app purchases [17].

Parents in our study took steps to restrict their children's access to devices or to information on devices. Many did not share their smartphone's password, meaning their children generally could not use the device without asking their parents. Parents from three families created separate user accounts for children on their home computers. This enabled children to use the computer and allowed parents to limit children's ability to access certain documents, files, and software. This suggests that parents recognize how to mediate children's technology use when the risk involves their own accounts or materials.

4.5.3 Privacy and Security Concerns Deferred to *Future* Time

Except for parents from two families who brought up specific concerns related to their children's self-presentation online, parents in our study did not identify privacy or security concerns about their children's online activities. One reason is that most did not see their children as engaging in activities that would raise those types of concerns. Many said their children were not interested in doing much online besides watch videos or play games:

> "He [a 6-year-old boy] just goes to his [websites], because again, it's like he's not interested in stuff that is not his age group right now. Because he'd be like, well I'm not supposed to do that and it's bad for me, and also it's not cartoons….I don't think he has the sense that there's much on there that could be harmful. I think mostly it's just that most other things are not interesting. He hasn't discovered the magic of endless YouTube yet" (Family X father).

Most parents in our study recognized this would change as their children grew up, though only one specifically mentioned that children would have a greater interest in privacy in the future. A mother from Family S said that when her 5-year-old son is older, "*He will want his privacy. Now he wants to be surrounded by, be near family.*"

Parents in our study also believed they would have to consider privacy and security more when their children had their own smartphones and used social media. They thought managing these concerns would require a balancing act:

> "I think it'll be a delicate balance of not being too intrusive but also I think there will be an element of earning trust and stuff in the beginning" (Family W mother).

Parents from a majority of families said they would consider using blocking, filtering, or monitoring software when their children were older and engaged in more online activities. They also said they would have more conversations with children about topics like creating strong passwords, not revealing personal information, not talking to strangers, avoiding bullying, and not viewing inappropriate content. What was clear overall is that parents were not focused on building foundational privacy and security skills until they perceived that their children's activities more clearly necessitated such action.

5 SUMMARY OF KEY FINDINGS

We summarize the key findings based on the three research questions that guided this work.

First, children in our study recognized certain components of privacy and security and applied this knowledge while going online, but younger children (ages 5-7) were much more limited in their knowledge and practices. They showed a basic understanding of how attributes and actors implicate privacy. Children under age 10 struggled to grasp concepts such as transmission principles. For most children, fear of punishment rather than concerns over privacy and security shaped their understanding of contexts for appropriate online information disclosure. Children in our study were understandably still learning how to make decisions and did not always demonstrate good judgment when discussing privacy and security concerns.

Second, children in our study demonstrated a small set of strategies to address privacy and security online, and parents played an important role. A few children identified strategies such as providing false information or restricting access to information as ways to protect privacy and security online. However, most said they would ask a parent if an unfamiliar or concerning situation arose online. Children in our study saw their parents as a trusted, reliable source of information, giving parents a clear opportunity to foster good privacy and security practices.

Third, parents in our study used mostly passive strategies to mediate children's online activities and largely felt that their children were too young to face privacy and security concerns. Parents primarily used passive techniques, such as setting boundaries or maintaining ambient awareness, to mediate their children's device use. A few expressed privacy concerns about children's online self-presentation, and many took steps to secure themselves from children spending money or accessing parents' information. Most parents in our study felt their children were not exposed to privacy and security concerns, even though their children searched for information online and, in some cases, used social media. Parents believed they might more actively mediate their children's device use in the future by, for example, using blocking, filtering or monitoring software or talking to their children about privacy and security online. Yet, helping children develop foundational skills early is essential to preparing them to manage the privacy and security risks they may face when they are teenagers.

6 DISCUSSION

In this study, we address an increasingly important but understudied topic: how children ages 5-11 conceptualize privacy and security online. Parents may think that conversations about privacy and security are not necessary until children grow older. However, we argue that helping children develop skills around smarter, safer online behaviors while they are young offers them a stronger foundation when they transition to adolescence and adulthood amid a rapidly evolving Internet landscape. Based on our findings, we discuss recommendations for helping children ages 5-11 develop such foundations to protect their privacy and security online.

6.1 Help Children and Parents Better Identify What It Means to Be Online and When Risks Can Emerge

Children in our study used Internet-connected devices to seamlessly weave the Internet into household life. Consequently, many children and some parents had difficulty identifying when they were online. This distinction will only grow blurrier as Internet of Things devices such as the Amazon Echo become more popular [22]. It is important to help children and their parents recognize (and remember) that use of these devices can raise privacy and security concerns. This suggests an opportunity for the development of resources to help children ages 5-11 and their parents identify what the risks are, when they are likely to occur, and with what devices. These resources could teach children about good practices for protecting their privacy and security online as well as why they should follow these guidelines in the first place.

The challenges that children (and parents) have defining what it means to be online underscores the importance of having these conversations early. Children should understand that tapping the Netflix app on a tablet, going to the Netflix website on a laptop, and telling the Amazon Echo to pull up Netflix on the TV all constitute going online. Several existing resources for children discuss the Internet or going online generally [11, 15, 16], but if children do not understand when they are or are not online, they may not recognize when to apply the lessons from such resources.

6.2 Use Contextual Integrity to Help Develop Educational Resources for Elementary School-Aged Children

While children in our study understood how the contextual integrity components of *attributes* and *actors* implicate privacy, they had a harder time understanding the role of *context* and *transmission principles*. Using contextual integrity as a guide, we suggest ways that designers can help strengthen children's understanding of these concepts, which will in turn help children develop the skills to manage their privacy and security online.

6.2.1 Help Children and Parents Build on and Extend Existing Knowledge using Contextual Integrity as a Guide

Actors: Existing research identifies six privacy and security risks that stem from children's use of Internet-connected devices: (1) inappropriate disclosure of information, (2) poor judgment when sharing information on social media, (3) exposure to inappropriate content, (4) stranger danger, (5) commercial data mining, and (6) normalization of surveillance [35, 37, 44, 47]. The families in our study recognized the first four but largely did not discuss the latter two. In fact, only two children stated that websites like YouTube can "*see*" what people do, recognizing that this affects their privacy while using the site.

We recommend the development of educational resources to help children understand that other *actors* are involved in online activities and that these actors affect people's privacy and security online. One way to integrate these lessons into children's everyday device use could be to create an online ad blocker for children to teach them about the entities involved in online activities. For example, a browser extension could explain to children that other *actors* (e.g., companies, website trackers) "watch" what people do online as part of providing the service. This "watching" offers benefits (e.g., the website remembers when a user has watched a particular video), but also raises concerns (e.g., a tracker on the website might tell other websites what videos a user has watched). The child-friendly ad blocker could show children how many trackers are on each webpage and could include interactive activities designed to help children learn more about how the Internet and World Wide Web operate. Integrating these educational resources into children's everyday online activities could help them internalize privacy and security concepts in a way that goes beyond a lesson in school.

Transmission Principles: Children in our study understood little about *transmission principles* and how the medium of communication affects the privacy of the information they share. Resources that teach children about how the Internet ecosystem works (i.e. what it means that a website "watches" you) may further lay the groundwork for children to better comprehend *transmission principles*. This would support their ability to learn about more complex privacy issues like data mining and surveillance.

Existing examples of ways to foster such understandings include the Berkman Klein Center's "The Internet and You" curriculum [18], which teaches children age 6-8 about privacy online, search engines,

and advertising, as well as "The Watchers," a privacy literacy game that researchers co-designed with children ages 8-11 [44]. We applaud these efforts and suggest, perhaps counterintuitively, that the development of resources focused more generally on how the Internet functions may complement these resources by helping children better understand how and why certain online activities raise privacy and security concerns.

Contexts and Norms: Children in our study understood that certain types of information can be sensitive, but they struggled to understand the *contexts and norms* around sharing information. Reminding children about information sensitivity as they interact with everyday apps can help them refine their understanding of *context*. For example, the website for PBS Kids,[3] a public broadcasting channel in the U.S., instructs children not to use any personal information (e.g., last name, address, personally identifiable information) when creating a username [41]. Rather than require children to set up security questions, which often use personal information, the site lets children select a "secret code" of three pictures. We recommend that apps and websites for children ages 5-11 incorporate learning opportunities that children can encounter through regular use of the service.

6.3 Encourage Parents to Scaffold Children's Development of Strategies to Address Privacy and Security Concerns

Our findings demonstrate that while children have developed some strategies to address privacy and security online, they largely rely on their parents for support. And while parents in our study did mediate their children's device use, they did not view their practices as addressing privacy or security concerns. Additionally, parents in our study used fairly passive strategies to mediate children's device use. They believed they would use more direct mediation in the future, when they perceived privacy and security risks for their children would be more salient. This contrasts the thinking of some experts, who find direct intervention to be privacy-invasive or ineffective for teenagers but appropriate for younger children [31].

We argue that a transition from parents' use of passive to more active mediation may be smoother if it takes place before adolescence, when children are more keenly focused on relationships with parents and adults [5]. Our findings show that children ages 5-11 rely on their parents for advice and guidance; teenagers, by contrast, do not communicate much with parents about their online risk experiences [53].

These findings suggest that parents may be missing opportunities to provide scaffolding for their children at a time when leveraging their zone of proximal development (ZPD) could significantly improve their privacy and security knowledge [7, 48, 50]. If parents more actively scaffold children's privacy and security strategies during stages where children are more focused on adult/parent relationships, children may be better prepared to address new types of privacy and security concerns when they reach adolescence and adulthood. This is important because today's children live in an increasingly connected world and will benefit from increased understanding and skills regarding privacy and security to build upon during adolescence.

Existing resources for parents focus primarily on older children. The U.S. Federal Trade Commission's Net Cetera guide [16] emphasizes the importance of communicating with children about online safety. But its suggestions for children under age 8 focus on supervision and parental controls rather than how to discuss privacy and security with children. Other resources such as the Family Online Safety Institute's Good Digital Parenting initiative[4] include a list of "can't-miss" opportunities to have conversations about online safety with children: when children receive their first phone, turn 13, and receive a driver's license [15]. These milestones lie far in the future for the children in our study. We suggest the development of resources to help parents understand how to discuss privacy and security concerns with their children before they enter adolescence.

To fit within children's ZPD, resources to support development of children's privacy and security strategies should encourage and facilitate children and parents working together, as our findings show

[3] http://pbskids.org/
[4] https://www.fosi.org/good-digital-parenting/

that children largely rely on their parents for guidance related to privacy and security online. Additionally, such resources for parents and children may be more successful if they focus on skill-building rather than minimizing privacy and security risks. Parents may overlook resources focused specifically on privacy and security, since they may not believe such resources are necessary for younger children.

Existing resources to teach children about privacy and security online include some components for parents. For example, the Berkman Klein Center's "The Internet and You" curriculum for children ages 6-8 includes parent handouts [18], and Google's "Be Internet Awesome" game for children ages 8-11 includes a parent pledge [11]. However, we suggest that resources for children age 5-11 should also give children the opportunity to apply strategies they learn [7]. For example, an app could show a video about strong passwords that a parent and child could watch together. Watching the video could unlock a secret messaging function in the app, and parents and children could work together to create a strong password to access the messaging feature. These kinds of resources can help facilitate conversations around best practices for managing privacy and security across *contexts* and with different *actors* in a child's everyday life.

6.4 Limitations and Future Work

This study's sample primarily includes families with highly educated heterosexual parents. While we did not ask participants about family income, their areas of residence and the prevalence of digital devices in children's home and school environments suggests these families come from the middle- or upper-middle class. In addition to the self-selection bias that accompanies interview-based research, the recruitment materials referenced privacy and safety. This means the parents in our sample may be more interested in the topic than an average family, though parental scores on privacy and security scales suggest that their privacy and security behaviors are close to average. Finally, the presence of parents and children in the vicinity while the interviews took place may have led participants to moderate their responses.

Future research should explore the privacy and security perceptions and strategies of lower-income families as well as families with different structures. Lower-income families may have less experience using digital devices, and families with structures that do not include two heterosexual parents may have to navigate different challenges. Additional research should measure parents' knowledge and habits related to privacy and security online and compare this to what their children are learning at home. Future work should also explore what children are learning about privacy and security at school. Comparing the habits of parents to those of children and comparing what children learn at home to what they learn at school could identify gaps that need to be addressed. This could also surface opportunities to foster greater privacy and security knowledge among children and parents.

7 CONCLUSION

In this paper, we presented the results of a qualitative study to understand what mental models children ages 5-11 have regarding privacy and security online. We also explored the strategies children and their parents use to address these concerns. We found that children have a reasonable understanding of some privacy and security components, but children ages 5-7 had some gaps. Children have some strategies to manage privacy and security online but rely heavily on their parents for support.

Parents use mostly passive strategies to mediate their children's device use, and they largely defer addressing privacy and security concerns to the future. Based on these findings, we recommend that parents can further enhance children's understanding of privacy and security online if they scaffold learning opportunities for children. Educational resources, including those built directly into existing website and apps, can take advantage of the contextual integrity framework to teach children how the Internet operates and what it means to be online. These resources should promote direct engagement between parents and children and should focus on helping children grasp why certain practices protect privacy and security online. Finally, parents may benefit from guidance on how to help children develop

good privacy and security practices before they reach adolescence. This can better prepare them to manage their privacy and security as adolescents and adults.

ACKNOWLEDGMENTS

We thank the family participants for their time. We thank Casey Fiesler and the organizers of the InfoSocial 2017 Graduate Student Conference at Northwestern University for their comments on an early draft of this paper. We also thank the anonymous reviewers for their feedback, which strengthened this paper. This work was supported by a Google Faculty Research Award.

REFERENCES

[1] Louise Barkhuus. 2012. The Mismeasurement of Privacy: Using Contextual Integrity to Reconsider Privacy in HCI. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 367–376.
[2] Lindsay Blackwell, Emma Gardiner, and Sarita Schoenebeck. 2016. Managing Expectations: Technology Tensions Among Parents and Teens. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, ACM, 1390–1401.
[3] danah boyd. 2014. *It's complicated: the social lives of networked teens*. Yale University press, New Haven.
[4] Tom Buchanan, Carina Paine, Adam N. Joinson, and Ulf-Dietrich Reips. 2007. Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology* 58, 2: 157–165.
[5] Duanne Buhrmester and Karen Prager. 1995. Patterns and Functions of Self-Disclosure During Childhood and Adolescence. In K.J. Rotenberg, ed., *Disclosure Processes in Children and Adolescents*. Cambridge University Press, Cambridge, UK, 10–56.
[6] L. J. Camp. 2009. Mental models of privacy and security. *IEEE Technology and Society Magazine* 28, 3: 37–46.
[7] Seth Chaiklin. 2003. The Zone of Proximal Development in Vygotsky's Analysis of Learning and Instruction. In A. Kozulin, B. Gindis, V.S. Ageyev, and S.M. Miller, eds., *Vygotsky's Educational Theory in Cultural Context*. Cambridge University Press, Cambridge, UK, 65–82.
[8] Malinda J. Colwell, Kimberly Corson, Anuradha Sastry, and Holly Wright. 2016. Secret keepers: children's theory of mind and their conception of secrecy. *Early Child Development and Care* 186, 3: 369–381.
[9] Common Sense Media. 2013. *Zero to Eight: Children's Media Use in America 2013*. Common Sense Media, San Francisco, CA.
[10] Lorrie Faith Cranor, Adam L. Durity, Abigail Marsh, and Blase Ur. 2014. Parents' and Teens' Perspectives on Privacy In a Technology-Filled World. *SOUPS*, 19–35.
[11] Pavni Diwanji. 2017. "Be Internet Awesome": Helping kids make smart decisions online. *Google*. Retrieved July 9, 2017 from http://www.blog.google:443/topics/families/be-internet-awesome-helping-kids-make-smart-decisions-online/.
[12] Andrea Düerager and Sonia Livingstone. 2012. *How can parents support children's internet safety?* London School of Economics, London, UK.
[13] Serge Egelman and Eyal Peer. 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ACM, 2873–2882.
[14] Lesley-Anne Ey and C. Glenn Cupit. 2011. Exploring young children's understanding of risks associated with Internet usage and their concepts of management strategies. *Journal of Early Childhood Research* 9, 1: 53–65.
[15] Family Online Safety Institute. *Three Teachable Moments*. Family Online Safety Institute, Washington, DC.
[16] Federal Trade Commission. 2014. *Net Cetera: Chatting with Kids About Being Online*. U.S. Federal Trade Commission, Washington, DC.
[17] Natt Garun. 2017. Amazon will soon refund up to $70 million of in-app purchases made by children. *The Verge*. Retrieved April 27, 2017 from http://www.theverge.com/2017/4/4/15183254/amazon-ends-appeal-refund-70-million-in-app-purchases.
[18] Paulina Haduong, David Cruz, Leah Plunkett, and Urs Gasser. 2016. *The Internet and You*. Berkman Klein Center for Internet & Society, Cambridge, MA.
[19] Alexis Hiniker, Sarita Y. Schoenebeck, and Julie A. Kientz. 2016. Not at the Dinner Table: Parents' and Children's Perspectives on Family Technology Rules. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, ACM, 1376–1389.
[20] Alexis Hiniker, Hyewon Suh, Sabina Cao, and Julie A. Kientz. 2016. Screen Time Tantrums: How Families Manage Screen Media Experiences for Toddlers and Preschoolers. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, ACM, 648–660.
[21] Donell Holloway, Lelia Green, and Sonia Livingstone. 2013. *Zero to eight: young children and their internet use*. London School of Economics, London.
[22] Mat Honan. 2017. Meet Amazon's New Echo Show: Alexa Is Watching. *BuzzFeed*. Retrieved June 27, 2017 from https://www.buzzfeed.com/mathonan/meet-amazons-new-echo-show-alexa-is-watching.
[23] Lori G. Irwin and Joy Johnson. 2005. Interviewing Young Children: Explicating Our Practices and Dilemmas. *Qualitative Health Research* 15, 6: 821–831.
[24] P.N. Johnson-Laird, Vittorio Girotto, and Paolo Legrenzi. 1998. *Mental models: a gentle guide for outsiders*. Retrieved from http://musicweb.ucsd.edu/~sdubnov/Mu206/MentalModels.pdf
[25] Amanda Lenhart. 2015. *Teens, Social Media & Technology Overview 2015*. Pew Research Center, Washington, DC.
[26] Sonia Livingstone. 2006. Children's Privacy Online: Experimenting with Boundaries Within and Beyond the Family. In R. Kraut, M. Brynin, and S. Kiesler, eds., *Computers, Phones, and the Internet: Domesticating Information Technology*. Oxford University Press, New York, NY, 145–167.
[27] Sonia Livingstone and Leslie Haddon. 2012. Theoretical framework for children's internet use. In S. Livingstone, L. Haddon, and A. Görzig, eds., *Children, Risk and Safety on the Internet: Research and policy challenges in comparative perspective*. Policy Press, Bristol, UK, 1–14.
[28] Sonia Livingstone, Leslie Haddon, and Anke Görzig, eds. 2012. Children, risk and safety on the internet: research and policy challenges in comparative perspective. Policy Press, Bristol, UK.
[29] Sonia Livingstone, Uwe Hasebrink, and Anke Görzig. 2012. Towards a general model of determinants of risk and safety. In S. Livingstone, L. Haddon, and A. Görzig, eds., *Children, Risk and Safety on the Internet: Research and policy challenges in comparative*

perspective. Policy Press, Bristol, UK, 323–337.
[30] Mary Madden, Sandra Cortesi, Urs Gasser, Amanda Lenhart, and Maeve Duggan. 2012. *Parents, Teens, and Online Privacy*. Pew Research Center, Washington, DC.
[31] Abigail Marsh, Lorrie Faith Cranor, and Julie S. Downs. 2017. *Experts' Views on Digital Parenting Strategies*. Carnegie Mellon University, Pittsburgh, PA.
[32] Melissa Mazmanian and Simone Lanette. 2017. "Okay, One More Episode": An Ethnography of Parenting in the Digital Age. *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, ACM, 2273–2286.
[33] 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. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, ACM, forthcoming.
[34] Megha Mohan and Kayleen Devlin. 2017. Fears over fake Bieber and Styles accounts. *BBC News*. Retrieved April 27, 2017 from http://www.bbc.com/news/blogs-trending-39670673.
[35] Kathryn C. Montgomery. 2013. Protecting Children's Privacy Online: The Battle Continues. *Human Rights* 39, 3: 6.
[36] Helen Nissenbaum. 2010. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, Stanford, CA.
[37] G. S. O'Keeffe, K. Clarke-Pearson, and Council on Communications and Media. 2011. The Impact of Social Media on Children, Adolescents, and Families. *Pediatrics* 127, 4: 800–804.
[38] Leysia Palen and Paul Dourish. 2003. Unpacking "Privacy" for a Networked World. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 129–136.
[39] Jessica A. Pater, Andrew D. Miller, and Elizabeth D. Mynatt. 2015. This Digital Life: A Neighborhood-Based Study of Adolescents' Lives Online. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ACM, 2305–2314.
[40] Gabriela Pavarini, Debora de Hollanda Souza, and Carol Kozak Hawk. 2013. Parental Practices and Theory of Mind Development. *Journal of Child and Family Studies* 22, 6: 844–853.
[41] PBS Kids. 2017. Frequently Asked Questions. Retrieved April 27, 2017 from http://pbskids.org/help/faq.html#good_username.
[42] Sandra Petronio. 2002. *Boundaries of privacy: dialectics of disclosure*. State University of New York Press, Albany.
[43] Chris Quintana, Brian J. Reiser, Elizabeth A. Davis, et al. 2004. A Scaffolding Design Framework for Software to Support Science Inquiry. *Journal of the Learning Sciences* 13, 3: 337–386.
[44] Kate Raynes-Goldie and Matthew Allen. 2014. Gaming Privacy: a Canadian case study of a children's co-created privacy literacy game. *Surveillance & Society* 12, 3: 414–426.
[45] Irving Seidman. 2013. Interviewing as Qualitative Research: A Guide for Researchers in Education & the Social Sciences. Teachers College Press, New York.
[46] H. Jeff Smith, Tamara Dinev, and Heng Xu. 2011. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly* 35, 4: 980-A27.
[47] Valerie Steeves, Trevor Milford, and Ashley Butts. 2010. *Summary of Research on Youth Online Privacy*. Office of the Privacy Commissioner of Canada, Ottawa, Canada.
[48] Lev Vygotsky. 1987. Zone of Proximal Development. Mind in society: The development of higher psychological processes 5291: 157.
[49] Rick Wash. 2010. Folk Models of Home Computer Security. In Proceedings of the Symposium on Usable Privacy and Security (SOUPS).
[50] James V Wertsch. 1984. The Zone of Proximal Development: Some Conceptual Issues. *New Directions for Child and Adolescent Development* 1984, 23: 7–18.
[51] Heinz Wimmer and Josef Perner. 1983. Beliefs about beliefs: Representation and constraining function of wrong beliefs in young children's understanding of deception. *Cognition* 13, 1: 103–128.
[52] Pamela Wisniewski, Haiyan Jia, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2015. "Preventative" vs. "Reactive": How Parental Mediation Influences Teens' Social Media Privacy Behaviors. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, ACM, 302–316.
[53] Pamela Wisniewski, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2017. Parents Just Don't Understand: Why Teens Don't Talk to Parents About Their Online Risk Experiences. *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, ACM, 523–540.
[54] Maxine Wolfe. 1978. Childhood and Privacy. In I. Altman and J.F. Wohlwill, eds., *Children and the Environment*. Plenum Press, New York, NY, 175–222.
[55] Yaxing Yao, Davide Lo Re, and Yang Wang. 2017. Folk Models of Online Behavioral Advertising. *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, ACM, 1957–1969.
[56] 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. *Proceedings of the 15th International Conference on Interaction Design and Children*, ACM, 388–399.

Received April 2017; revised July 2017; accepted August 2017