Child Safety in the Smart Home: Parents' Perceptions, Needs, and Mitigation Strategies

KAIWEN SUN, School of Information, University of Michigan, USA
YIXIN ZOU, School of Information, University of Michigan, USA
JENNY RADESKY, Department of Pediatrics, University of Michigan Medical School, USA
CHRISTOPHER BROOKS, School of Information, University of Michigan, USA
FLORIAN SCHAUB, School of Information, University of Michigan, USA

Concerns about child physical and digital safety are emerging with families' adoption of smart home technologies such as robot vacuums and smart speakers. To better understand parents' definitions and perceptions of child safety regarding smart home technologies, we interviewed 23 parents who are smart home adopters. We contribute insights into parents' perceptions of the physical and digital safety risks smart home technologies pose to children, and how such perceptions formed and changed across three phases. In acquiring smart home devices, parents already considered whether the device could cause physical harm to their children or pose privacy and security risks. Once children become active users of smart home technologies, parents however reported encountering unanticipated physical safety risks and digital safety issues (e.g., exposure to unsuitable content) that required their mitigation strategies. As their children grow up, parents further expressed the need to shift attention from physical safety to digital safety. Parents' safety perceptions influence how they involve children in smart home interactions and implement mitigation strategies, such as restricting access to certain devices and using parental controls. We identify six factors that shape parents' perception and evaluation of smart home safety risks to children, including parenting style, parents' tech-savviness, parents' trust in tech companies, children's age and developmental differences, news media, and device characteristics. We provide design and policy recommendations to better protect children's safety in the smart home environment.

CCS Concepts: • **Security and privacy → Social aspects of security and privacy**; *Usability in security and privacy*; • **Human-centered computing → Ubiquitous and mobile devices**; • **Social and professional topics → Children**.

Additional Key Words and Phrases: Smart home technologies; child safety; parenting; child-centered design.

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

1 INTRODUCTION

Children are sensitive to and dependent upon their care-giving environments. In particular, creating a nurturing and safe home environment is critical to children's family life experiences [17]. Many

Authors' addresses: Kaiwen Sun, kwsun@umich.edu, School of Information, University of Michigan, Ann Arbor, MI, USA; Yixin Zou, yixinz@umich.edu, School of Information, University of Michigan, Ann Arbor, MI, USA; Jenny Radesky, jradesky@umich.edu, Department of Pediatrics, University of Michigan Medical School, Ann Arbor, MI, USA; Christopher Brooks, brooksch@umich.edu, School of Information, University of Michigan, Ann Arbor, MI, USA; Florian Schaub, fschaub@umich.edu, School of Information, University of Michigan, Ann Arbor, MI, USA.

2573-0142/2021/10-ART471. https://doi.org/10.1145/3479858

parents have adopted smart home technologies — sensors, interfaces, appliances, and devices to enable home automation through localized and/or remote control [16] — for the purposes of security, convenience, or energy saving [1, 47, 70]. As a result, many children grow up in home environments filled with smart home technologies, ranging from smart speakers, smart locks to robot vacuums, that are designed by adults and usually for adults. Past research has surfaced issues of usability [9], privacy [37, 58], and security [61, 109] in various use cases of smart homes involving children.

Meanwhile, child physical safety is a significant focus of parenting young children as unintended injuries are a leading cause of child morbidity [44] and mortality [81]. While prior research demonstrates the importance of ensuring physical safety in the home environment [44, 81], child physical safety risks have not been studied in depth with regard to smart home technologies. Anecdotal evidence suggests that parents are concerned about the possibility that a vacuum cleaning robot could run over young children's toes [90], or battery compartments of a smart button might pose choking hazards [91]. Such anecdotes indicate that certain smart home technologies could pose physical safety risks given that they are physical objects situated in the home environment, often in close contact with children. Meanwhile, the Internet-connected nature of smart home technologies indicates potential digital safety risks to children, and little is known about how parents might perceive and deal with these physical versus digital safety risks differently.

Our research provides a deeper understanding of how parents conceptualize the physical and digital safety risks in children's interactions with smart home technologies and their corresponding mitigation strategies. Specifically, we conducted semi-structured interviews with 23 parents who are adopters of various smart home technologies with children from young toddlers to preteens (1-11). We aimed for a wide range for children's age to ensure we get diverse perspectives of how children interact with smart home technologies. Our study addresses the following research questions:

(1) What are parents' perceptions of children's safety in the context of smart home technologies, and what factors shape such perceptions?
(2) What approaches and strategies, if any, do parents adopt to mitigate perceived child-safety risks?

We find that parents' perceptions of smart home safety risks included both physical and digital aspects and evolved in three phases. When deciding to purchase smart home technologies (phase 1), most parents consider whether certain technologies might pose obvious physical safety, privacy, or security risks for their children. As their children became active users of the acquired smart home technologies (phase 2), parents discovered safety risks they had not considered and re-evaluated children's use cases, such as how children's improper use of the technology may lead to physically unsafe situations and how children might be exposed to unsuitable digital content. Parents discussed the need for further adjustment as their children grow up (phase 3), with an increased focus on digital safety risks.

As their perceptions and safety concerns changed across the three phases, parents discussed making reactive decisions based on children's smart home experiences to protect children's physical and digital safety. For instance, parents became selective of the smart home technologies children are allowed to access, adjusted commands and controls children could use, or leveraged parental control features if available.

We identify multiple factors that influence parents' perceptions and mitigation strategies toward smart home safety risks to children, including parenting style, parents' tech-savviness, parents' trust in tech companies, children's age and developmental differences, news media, and device characteristics. We discuss how our findings relate to and build on existing literature, as well as implications for design and public policy to better support children's safety in smart homes.

2 RELATED WORK

We review existing work on child safety issues in the physical and digital world, parents' role in mitigating child safety risks, and the adoption of smart home devices.

2.1 Children's Safety in the Physical and Digital World

Prior research suggests that safety is an intersubjective concept subject to social construction, collective agreement, and socialization [110]. Although objective danger exists, children develop safety awareness through observing caregivers' cues and responses [83, 92, 94]. While the home environment helps children develop a sense of safety and security [80], unintentional injuries often happen to children at home.

Many factors contribute to child home safety risks. Children have immature cognition and are unaware of or tend to ignore danger [87]. Children's age and compliance to home safety rules also determine their likelihood of getting into accidents: those who are younger or ignorant of safety rules are more likely to get injured [23, 66]. As for parents, lower educational and socio-economic backgrounds have been shown to increase safety risks for children [59, 65]. Parents' attitudes and behaviors toward home safety such as beliefs in fate, tolerance to risk, and training in children's safety practices are considered relevant to home accident prevention [48, 62, 63]. As for the home environment, a physical setup with lots of noise, disorder, and easy access to hazards increases children's risk of injuries [59, 65, 67, 73]. When it comes to the digital world, prior research suggests that young children (5–8 years of age) have minimal understanding of technical and social aspects of the Internet or its risks [104, 105]. Parents' concerns about children's use of the Internet center on privacy invasions [57], cyberbullying [54], addiction [50], and explicit content [31, 54].

Regarding smart home devices, past research has primarily focused on privacy and security issues that could expose families' sensitive information [45, 71], usability issues that diminish user experiences [7, 102], and the lack of granular privacy controls that could cause tensions among multiple users [89, 99, 108]. More specific to children, Internet-connected toys such as My Friend Cayla raise privacy concerns for parents [61] as these toys introduce opportunities for malicious attacks (e.g., hacking the toy to operate a smart lock using voice commands) [24, 68]. Another example is smart security cameras installed in children's bedrooms, which could be hacked to spy on, scare, or harass children [93].

Nonetheless, little research has examined safety risks of smart home technologies in households involving children. Smart home technologies — by residing in the home space while serving as portals to the Internet and bridges amongst different devices — could amplify existing safety risks and introduce new risks to children. Our study investigates how parents perceive and react to smart home safety risks to children, and in particular, whether parents associate smart home safety risks with other child safety risks in the physical and digital world.

2.2 Parents' Role in Children's Physical and Digital Safety

Parents play a significant role in managing risks for children by baby proofing the home environment [25, 44], supervising children [65], and teaching children about risky situations and how to avoid hazards in the physical world [72]. Gärling and Gärling [35] found that parents attempt to manage children's injury risks by teaching them how to behave safely by the time children reach three years of age. Common teaching strategies include explanations, establishing rules, and modifying behaviors through rewards or punishment [63]. Parenting style also influences how parents teach children home safety rules and how effectively the rules reduce children's injury risks. For instance, permissive parents who impose less control on their children tend to explain, rather than command, rules about home safety [63]. Such a parenting style might increase young children's safety risks due to a lack of clear rules on what behaviors are acceptable [63] and a lack of opportunities for children to internalize behaviors that need self-regulation [60].

Past research has also examined parents' strategies to minimize their children's online risks in the digital world. The EU Kids Online network [54] identified common approaches used by parents, including active mediation of Internet use and Internet safety (e.g., discussing online activities and safety practices with children), restrictive mediation (e.g., setting rules for Internet use); monitoring Internet use; and technical mediation (e.g., using parental controls to constrain use). Among these strategies, studies have found that parents with more advanced digital skills tend to use active mediation, whereas parents with lower digital skills tend to use more restrictive mediation strategies or implement technical restrictions [54, 69]. Our study examined parents' strategies to mitigate perceived safety risks when children use smart home technologies — which pose a hybrid of physical and digital child safety risks by physically being in the home environment while also being connected to the digital world.

2.3 Smart Home Device Adoption and Evaluation

Consumers' purchasing experience consists of pre-purchase evaluation, purchase, consumption, and post-consumption evaluation [11]. Karapanos et al. [41] highlighted the temporality of user experience, i.e., how the quality of user experience develops from short-term pleasures in early stages to reflections on the product's influence in prolonged use. Their framework identifies consumers' adoption, acceptance, and evaluation of products as phases of a reflective process [41]. Regarding user interactions with smart home systems, Jakobi et al. [38] identified a four-phase process from system setup, configuration, daily use, to reconfiguration and extension.

Throughout different phases, consumers' evaluations of digital products are influenced by numerous factors [41]. Lau et al. [51] found that during pre-purchase evaluation, convenience and a mindset of wanting to stay current with technology were two primary motivators for adopting smart speakers; price, brand, and compatibility were secondary. Privacy, security, and trust in brands and companies were also key influencers on people's willingness to adopt smart home devices [6, 51]. Powers et al. [74] found that social media news affected people's purchase behaviors around consumer goods such as electronics and groceries. The purchase decision further depends on the user's identities or preferences: energy-sensitive users look for smart home products with energy saving features [19, 53], tech enthusiasts value devices that enhance home control and automation lifestyle [16, 70], and parents value devices that support family use [22].

In the post-consumption phase, consumers evaluate their experiences while reflecting on their original considerations toward the product, and such reflection affects their overall satisfaction [4]. Emami-Naeini et al. [28] found that many participants in their study did not consider privacy and security as a determining factor before purchasing smart home devices, but came to realize privacy and security issues later on through using the device, news reports, and peer influences. Multiple users sharing the same smart home device may pose issues for access-control mechanisms [33, 88, 109] and negatively impact the post-consumption experience [106–108]. For instance, Choe et al. [14] uncovered tensions among household members due to different comfort levels with in-home sensors.

To the best of our knowledge, our study is among the first to examine parents' consideration of children's safety across the pre-and post-purchase phases of smart home technologies. Our study contributes insights on how parents factor child safety into their evaluation of smart home technologies. Specifically, we find that parents focused on physical safety, privacy, and security aspects in purchasing the device, identified additional safety issues such as exposure to unsuitable content during children's use, and paid increasing attention to digital safety as children grow up.

3 METHODS

To explore how parents perceive child safety in smart homes and how parents mitigate perceived safety risks, we conducted semi-structured interviews with 23 parents who (1) are owners and users of smart home technologies (e.g., smart speakers, smart security cameras, and smart doorbells) and (2) have children in the age range of 1–11 years who had experiences using smart home technologies. We decided to interview only parents, not children, as parents are usually adopters and pilot users of smart home technologies [33, 46] who are in control of their children's experiences. Most participants owned a variety of smart home devices, so they might have an enriched experience with smart home technologies and more awareness of different device-specific safety aspects than the general public. We recruited parents with children from young toddlers to preteens to explore if parents' perception of safety issues depends on children's age.

While we initially planned to conduct in-home interviews with parents to contextualize their smart home device placements and interactions, the COVID-19 pandemic made us opt for virtual visits instead. When piloting virtual visits, we asked the interviewee for a virtual tour as they held the camera to show us around their places while pointing out specific smart home technologies. However, these virtual tours turned out to be distracting and technically challenging to stay connected while providing little additional insight over the interview component. As a result, we decided to conduct remote interviews without virtual tours, accepting the drawback that we would have to rely on participants' self-reports without being able to see their home environment. Remote interviews however allowed us to recruit a geographically diverse sample across the US and Canada. We conducted our interviews from June to August 2020 through video calls with parents across the United States (US) and Canada (CA). Our study was deemed exempt from oversight by our university's Institutional Review Board (IRB).

3.1 Interview Protocol

Our interview protocol consisted of three parts: (1) smart home use and parents' mental models of smart home safety, (2) parents' perception of their children's smart home use and interactions in relation to safety, and (3) potential issues regarding children's use of smart home technologies and corresponding mitigation strategies from parents. We sequenced the interview questions in ways that create opportunities for parents to bring up safety issues on their own before we asked explicitly about safety and other specific concerns. The full interview protocol is provided in Appendix A. Since the interviews were semi-structured, we sometimes skipped questions listed in the protocol if parents had already answered them in a previous question or in their comments during the course of the interview.

In Part 1, we invited parents to describe both theirs and their children's smart home technology ownership, placement, and use. We then indirectly elicited parents' perceptions of smart home safety by asking about factors they considered before purchasing smart home technologies, whether they considered children's use in making purchase decisions, and what impacts smart home technologies could have on their children in their opinion. By doing this, we hoped to understand whether parents would intuitively bring up safety-related topics in discussing their children's use of smart home technologies. If parents mentioned safety-related considerations, we asked them to discuss specific safety concerns to gauge parents' perception of smart home safety risks.

In Part 2, we tried to further contextualize how parents perceived their children's smart home use and interactions. We asked about children's access to and control of smart home technologies, whether parents allow or limit children's access to certain smart home technologies and why. To learn about children's awareness of potential smart home safety risks from parents' perspectives, we asked parents if they felt comfortable leaving their children alone to operate smart home technologies, and if there was anything they disliked or were concerned about regarding their children's interactions with smart home technologies. If parents had not brought up safety-related topics by this point, we asked more directly about what they considered safe or unsafe regarding smart home devices, and which devices were safe or unsafe for their children in their opinion. We deliberately did not define 'safety' to elicit parents' own interpretations of what safety means in smart home contexts.

In Part 3, we asked parents whether their children have showed any concerns, challenges, or issues when interacting with smart home technologies, whether there were disagreements between parents and children in using the technology, and how parents mitigate issues related to safety. Because parental rules are a critical factor related to children's injury risks [66, 67], we asked whether and what rules parents established for their children's interaction with smart home technologies and how children reacted to these rules. We concluded the interview by asking parents if they had any suggestions regarding safer smart home technologies for children, such as desired features and functionalities.

ID	Ctry.	Child Age	TV	Speaker	Thermo.	Camera	Light	Switch	Lock	Door	Doorbell	Vacuum	Baby Monitor
P1	CA	18m, 4y	●			○		●		○			●
P2	US	9y, 12y	●		●				●				
P3	US	9y, 11y	●	●	○	●	○	●	●	●	●		○
P4	US	9y, 11y	●	●			○	○	●	○	●	●	
P5	US	5y, 7y	●	●	○	○		●	●	○	○		
P6	US	7y	●	●	○		●		○				
P7	US	7y, 8.5y	●		○	○	●	●	●	○			
P8	US	2y	○	●	○	○	●	○	○			●	○
P9	US	7y, 9y	●	●	○		●	●	●	○			
P10	US	8y, 9y	●	●		○		●			●		
P11	US	5y, 7y	●	●	○			●	●	●			
P12	US	2y, 5y, 8y, 10y	●	●	○	●	●	●			●	●	
P13	US	4y	●	●	●	○	●	●	●	○	●		○
P14	CA	2y, 4y	●	●	○	○	●		○		○	○	
P15	CA	8y, 8y	●	●	○	○	●	●					
P16	US	2y, 6y	○	●	○	○	●			○			
P17	US	3y, 6y	●	●	○	○	●				●		●
P18	CA	2y, 4y, 7y	●	●	○	●	●			○			●
P19	CA	5y	●	●	○		●	○				●	
P20	US	9y	●	●	○	○	●	●	●			○	
P21	US	2m, 8y, 10y	●	●		●				○	●	●	
P22	US	7m, 5y, 7y	●	●		●	●	●	●	●	●		○
P23	US	2y, 5y, 7y	●	●	○	○	●		●	○	●	●	

Table 1. Participant Demographics with Smart Home Devices (●: smart home device used by children; ○: smart home device used by parents but not children).

3.2 Participant Recruitment and Demographics

We recruited prospective participants through postings on Reddit, Craigslist and convenience sampling. We decided to use Reddit as the main recruitment platform since (1) Reddit provides a concentrated place to reach a regionally diverse sample [13], and (2) Reddit hosts several large parenting communities where parents can ask questions anonymously [2, 3]. With permissions from moderators, we posted recruitment messages in both parenting (e.g., r/parenting) and smart home (e.g., r/home automation, r/homekit) related subreddits. The recruitment message asked for parents who had children aged 1-11 years and multiple smart home devices. The recruitment message invited parents to share their children's interactions and experiences with smart home technologies, without mentioning safety explicitly. The recruitment message also included a link to a screening survey (see Appendix B), which captured parents' smart home device ownership, children's interactions with the devices, and children's age as primary inclusion criteria. Since we considered parents' income and educational level less related to our study focus, we did not collect such data in the screening survey. We then selected parents for the interview based on screening survey responses. The interview lasted 52 minutes on average, and each participant received a $25 check upon completing the interview.

For the 23 parents we interviewed (see Table 1), 18 were from the US and five from Canada. All parents owned at least three types of smart home devices, several parents reported having multiple devices of the same type that were placed in different rooms in their home. During the interview, most parents self-identified as tech-savvy owners and users of smart home technologies as a result of their tech-related occupation or hobby.

3.3 Data Analysis

The 23 interviews were conducted and recorded via Zoom with automatic transcription. Three team members reviewed all interview transcripts and made corrections as needed. One researcher went through all transcripts and created analytic memos to identify themes and categories for the initial codebook [82]. Together with another researcher, they reviewed several transcripts and iteratively refined the codebook by clarifying code definitions and resolving disagreements. Next, the two researchers individually coded the same six transcripts, compared coding results and adjusted the codebook in multiple rounds until reasonable inter-rater reliability was achieved (Cohen's κ = .77). One researcher then coded all 23 transcripts using the final codebook.

The final codebook (see Appendix C) consisted of 65 codes in five categories, including a combination of descriptive codes (e.g., child-proof smart home technologies), process codes (e.g., parental mediation strategies), concept codes (e.g., definition of smart home technologies), value codes (e.g., children's perception of smart home technologies), and causation codes (e.g., children's reactions to parental rules) [82].

3.4 Limitations

First, it is likely that some parents might have exhibited social desirability bias [30], as they sought to demonstrate themselves as responsible parents who care about their children's safety after figuring out the study's goal even though their parenting style is more complacent and relaxed.

Second, we did not collect parents' demographic information such as income and education level, which limits our ability to further characterize our sample. We learned through interactions with parents during the interview that most parents described themselves as tech-savvy due to tech-related occupations or personal interest. Thus, our findings provide a snapshot of a small sample of parents who are generally familiar with technologies. Future studies should study larger and more diverse groups of parents with different income, educational background, and familiarity with technologies.

Third, we recruited parents only from the US and Canada. Parents in other countries might have different perceptions of child safety in smart homes due to different cultural norms.

Fourth, our study focused on parents' perspectives since parents tend to be smart home adopters in charge of their children's access and use [33, 46]. However, parents' perspectives may not accurately reflect children's own perceptions toward smart home safety. Future work should study

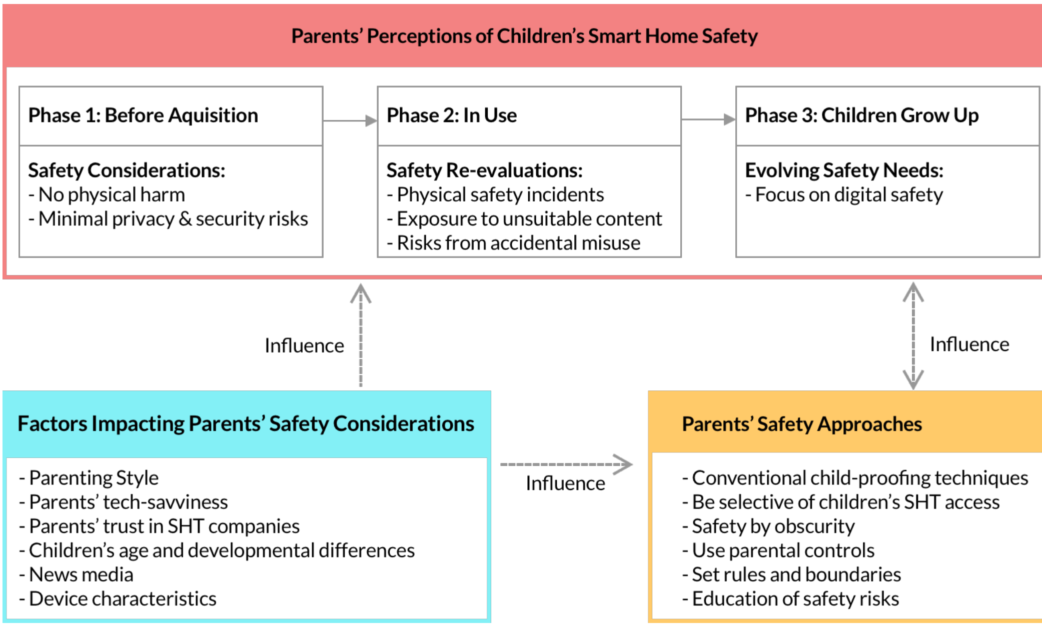

Fig. 1. A diagram of parents' perceptions of and approaches to children's smart home safety in relation to the factors (SHT = Smart Home Technologies).

how children conceptualize smart home safety, as well as how children and parents interact with and through smart home technologies using observations to provide further insights and reveal potential tensions between children's and parents' perspectives.

4 FINDINGS

Overall, we found that parents considered both physical and digital child safety risks with regard to smart home technologies. We identified three phases over which parents' perceptions of these safety risks evolved (see Figure 1). The evolving safety risk perceptions further influenced parents' decisions and mitigation strategies regarding their children and smart home technologies. Before purchasing or acquiring smart home technologies (phase 1), parents primarily focused on avoiding devices that could cause physical harm to children or had obvious privacy and security risks. As children started to use smart home technologies (phase 2), parents reactively re-evaluated safety risks after observing their children's usage patterns and became aware of how devices could expose children to unsuitable content or lead to physically unsafe situations. Parents discussed the evolving safety needs as children grow up (phase 3), and they became more worried about children's digital safety in smart homes. Accordingly, parents' mitigation strategies against perceived safety risks differed in the three phases, from avoiding purchasing certain smart home technologies (phase 1), being selective in children's access to devices and enforcing safety use guidelines (phase 2), to planning on educating their children about digital safety risks (phase 3). We next discuss our findings for each phase in more detail (Section 4.1 to 4.3) before summarizing six factors we identified that influence parents' considerations around smart home child safety (Section 4.4). To enhance children's safety and overall user experiences in smart homes, parents further suggested improvements in parental controls design and desired more transparency and accountability from tech companies (Section 4.5).

4.1 Phase One: Safety Considerations Before Device Acquisition

When considering the purchase of smart home devices, most parents reported being vigilant about children's smart home safety as they discussed initial safety concerns toward certain smart home technologies and associated risks. Parents stated that they would avoid certain smart home technologies that appeared to pose privacy and security risks for their family, might create physical harms to children, were branded by distrusted companies, or did not seem suitable for their children's age.

4.1.1 Privacy and security concerns. Most parents recognized that children's smart home safety is closely linked to privacy and security. Parents identified privacy and security risks from certain cloud-based devices such as security cameras, smart locks, and smart speakers. To mitigate these risks, parents either ruled out purchasing such devices, or put a lot of thought into choosing the device's brand and properly incorporating the device into their smart home systems.

Concerns over cloud-based security cameras. Most parents who expressed concerns about cloud-based security cameras mentioned the possibility of cameras being hacked and exposing their children to strangers' surveillance or contact; this was possibly due to some highly publicized cases before we conducted the interview [93]. Prior work suggests that users' distrust in tech companies and disbelief that their data would be handled properly hinder smart home device adoption [51, 103]. Similarly, we found that a few parents avoided certain security camera brands due to negative news reports. For instance, P13 said they deliberately decided not to use Motorola baby monitors because they had heard *"horror stories"* about the product getting hacked. Both P9 and P10 mentioned avoiding the Ring camera due to privacy issues and security breaches they had heard about the product. P6 noted a general skepticism toward any Internet-connected cameras:

> *"I don't like the idea of any camera that is accessible by any network in my home . . . They can see you and your home, and someone can activate that without knowing it. I just feel like it's very insecure, and . . . the [news] came out about all those cameras that were getting hacked. People were saying and doing terrible things through them. That was . . . another brick in the wall convincing me to have absolutely no cameras."*

P14 chose to have a security camera that was disconnected from the Internet and intentionally avoided putting it in the child's room. The action originated from what they learned from the news and their distrust in certain tech companies:

> *"If I don't trust that I have control of that thing, that would be the biggest red flag for me . . . I am not as comfortable with [the camera] given . . . all the current news and questions about the tech companies and access to data. The camera that I do have is inside the house . . . The video is stored on a hard drive and I have access to it from there . . . I don't necessarily want anyone else looking at my kids while they're sleeping."*

Concerns over smart locks. Some parents were skeptical about smart locks, mostly because they envisioned serious physical consequences if the smart lock was compromised. P10 shared that the locks in their home were all manual, as they were concerned that a smart lock could malfunction and unlock itself.

P11 explained why they specifically decided to get a Bluetooth-based smart lock:

> *"I'm not thrilled with the security implications of connecting the door lock to the Internet. If it's on Bluetooth only, then there's kind of 'less can go wrong' from a security perspective . . . [Considering that] anyone on the planet can open my front door [if I had an Internet-connected lock] . . . I wanted to keep it off the Internet."*

Tolerance of smart speakers' privacy risks. Nearly all parents had at least one smart speaker in their household. Most parents appeared to be aware of privacy risks associated with smart speakers but expressed tolerance to such risks. P22 shared:

> *"Most of the privacy [issues] that I would be worried about has to do with the speakers. You can obviously take user data for advertising through it, but even then, I don't think it puts anybody in jeopardy or anybody at risk."*

However, P1, a software developer with technical knowledge of Internet-connected devices' vulnerabilities, expressed stronger concerns and considered smart speakers unsafe for their children:

> *"What's coming to my mind is … smart [speakers with] videos, and especially devices that can make calls … It concerns me that my kids might communicate with somebody that I am unaware of … I don't want random people to be able to call the device, and I don't want my children to be able to call random people … I want to basically moderate who can and can't communicate with the device and by proxy my child."*

4.1.2 Device characteristics posing physical threats. In discussing factors they considered before purchasing smart home technologies for children's use, some parents mentioned physical safety concerns triggered by certain device characteristics. Several parents mentioned deliberately staying away from smart devices with motors (which produce heat) or lack product certifications (e.g., CE [96] or UL [98] certification). Parents viewed these features as potential physical safety threats and associated them with traditional home safety issues such as burns and injuries. P1 explained their concerns about smart technologies with heating functions:

> *"[I would not even consider] a smart heater … You'd be insane to build a smart heater, that's a great way to have somebody burn their house down and sue [the manufacturer] into oblivion … There [aren't] any physical things with motors or things with heaters [in our house]."*

P7 identified UL certification as a key indicator of a physically safe smart home device:

> *"Anything that needs to plug into main power absolutely has to be UL certified. End of story. Because then at least there's a basic understanding that it's probably been tested and it's probably not going to explode in the middle of the night."*

Overall, in phase 1 parents formed basic safety requirements for smart home technologies and considered them in the purchase decisions, such as minimal privacy and security risks and no potential for physical harm.

4.2 Phase Two: Safety Reflections and Re-evaluations During Use

Karapanos et al. [41] highlighted that users' evaluation of digital products is an ongoing and reflective process throughout adoption and use. Similarly, we observed that although parents considered certain safety risks before purchasing smart home devices, they later realized additional safety risks once their children started interacting with the device. Most parents mentioned that their children were unaware of or unable to fully understand smart home related safety risks. Thus, keeping children safe required constant effort and various strategies, such as child-proofing the smart home environment, limiting children's access to certain smart home devices, and establishing rules for safe use.

4.2.1 Safety issues in children's smart home use. Many parents described that their children had not yet developed awareness of smart home related safety risks due to children's young age and limited access or use. As parents described their children's smart home use, some shared physical safety incidents, some foresaw digital safety issues, and others worried about safety risks as a result of children's improper handling of the device.

Children's limited smart home safety risk perceptions. While parents strove to provide a safe smart home environment for their children, many said their children did not seem to be aware of safety risks associated with smart home technologies. Other parents did not think conversations about safety were necessary, as their children's smart home use had been supervised and limited to non-critical devices (e.g., smart lights) or devices disconnected from the Internet. As P16 discussed:

> *"I don't think [my kid] cares about bad actors on the Internet in terms of accessing things and compromised systems that go beyond her ... Our kids always have close adult supervision, whether it's my wife or our nanny."*

Some parents mentioned their children were aware of online safety risks, which may or may not apply to smart home contexts. P15 thought that their children understood the basic meaning of hacking but not in the context of smart home devices such as cameras being hacked. Similarly, P11 said their child understood that there are *"bad people online"* but not what risks might be:

> *"He probably has ... a real fledgling awareness of 'there are other people online and they're not always friends' ... I don't think [children] have any real concern about the scary stuff [such as news of smart home devices being compromised] that we read about."*

P13 considered it unsuitable to teach their four-year-old about smart home safety risks, which might scare the child as he was just starting to develop an understanding of the digital world:

> *"I don't think [the conversation] would help at this point ... I think it would actively hurt him. He's four, he likes to watch cartoons, he's starting to have vivid dreams ... and I don't necessarily want him thinking that his house, which is his safe area, could potentially turn against him."*

A few parents, usually with slightly older children, mentioned having conversations about smart home safety with their children but did not think that their children had an in-depth understanding. P12 said their children were taught to stop the smart speaker right away if it started *"playing music that sounds inappropriate."* P2 mentioned that their nine- and twelve-year-olds knew the smart lock's passcode and understood that they were *"not allowed to give out the code,"* but P2 also suspected that the children probably just treated it as a key without knowing much about related safety issues. Having experienced identity theft, P20 taught their nine-year-old the importance of protecting personal information online:

> *"We told him about [the identity theft experience] and he knew how stressful that was ... We got it all resolved, but it took a lot of work to resolve ... He saw how stressful that was ... So I think he understands the importance of protecting [his] identity and information."*

Physical safety incidents. Multiple parents of young children shared physical safety incidents that involved smart robot vacuums. P14 described:

> *"[The smart vacuum] was breaking. I had to get a replacement part to get it to detect people again ... I started the vacuum cleaner and walked away from it ... and it ran over her toes. It's not that heavy. It was just sort of an annoyance for her."*

P8 shared that *"the [vacuum] robot scared the dog, and the dog ran right past my son and spun him around."* Similarly, P12 mentioned that the smart vacuum could cause *"chain reactions"* that would pose safety hazards, such as by getting *"tangled in some wires and knocked stuff off the table"* which could accidentally hurt their children.

Children's exposure to inappropriate content. Compared to physical safety concerns with smart robot vacuums, smart speakers raised different safety concerns. Many parents reported that their children used smart speakers to ask questions, watch videos, or control other smart home devices such as lights and doorbells. Some parents worried about smart speakers exposing children to unsafe content. Such risk might originate from young children's struggles with pronouncing or spelling words correctly when asking questions. As P11 described:

> *"With a smart speaker, you can ask it all kinds of questions and maybe if you mispronounce something, you get something else that's more adult . . . I have seen the video where some kid asks and ends up getting sex toys . . . They could end up shopping for something like that by accident."*

Parents with older children were concerned about their children deliberately using smart speakers to access inappropriate content. P4 said:

> *"Sometimes [children] have this friend come over and he likes to try to get Alexa to play the music that I wouldn't let them listen to because the lyrics are unsafe . . . the content is [unsafe]."*

Furthermore, children could run into undesired experiences when the smart speaker is shared by multiple family members. P18 mentioned that their child accidentally came across child-inappropriate content in this way:

> *"[The smart speaker] will continue to play the last thing that was playing . . . So I'd be listening to something that has grizzly details and really not kid appropriate . . . Our seven year old [accidentally resumed it] and he would immediately tell it to stop and run away because he's very scared of being scared."*

P23 pointed out that such safety risks were not unique to children's use of smart speakers, *"but [smart speakers] maybe create more opportunities [for children to be exposed to inappropriate content]."* Specifically, the voice interaction with centrally-placed devices brings potentially inappropriate information closer to the child than when it can only be accessed via computers, phones, or tablets that can be removed from children's reach.

Potential safety risks from children's device use. Many parents said their children could use the smart speaker to control other smart home devices (e.g., lights) and automation (e.g., dinner mode) through voice commands or through the speaker's display interface. With such access, some parents worried that children's accidental misuse or mischief could create safety issues. P20 gave their nine-year-old full access to the smart home controls because they wanted the child to be part of the smart home experience. Nonetheless, P20 was frustrated by Google Home lacking *"the ability to limit the devices that [the child] has control over."* For instance, P20 had a smart water heater linked to the Google Home. To P20's knowledge, there was no way to prevent the child from accessing the water heater while still keeping the access to other less dangerous devices — this situation raised concerns that the child might use voice commands to activate the smart water heater:

> *"I don't want him controlling [the smart water heater] . . . He could burn himself, he could burn us . . . Let's say I'm in the shower and he tells the system to raise the temperature to 150 degrees . . . That's why I would prefer to be able to just block his access from something like that [but I can't]."*

Several parents further raised concerns about the safety implications of automated garage doors that could be controlled via smart speakers. P20 worried that their child, with full control access to the smart home system, might leave the garage door open, which could put the child at risk if left home alone. P16 described that their children were too young to understand that the garage door was not something to play with:

> *"I wouldn't want my kids to be silly and say, 'Alexa open the garage door' . . . Kids don't have a fully developed prefrontal cortex to . . . know [they] shouldn't play with the garage door . . . [They would] basically make it a game where [their] little brother runs underneath it as they close it."*

4.2.2 Parents' mitigation strategies. Parents shared various preventative and reactive mitigation strategies in response to safety concerns: conventional child proofing techniques, keeping young children under close supervision when they interacted with smart home devices, limiting what devices children had access to, and using devices' built-in parental control features if available.

Conventional child-proofing. Nearly all parents who child-proofed smart home devices when their children were younger mentioned common child-proofing approaches to prevent physical safety risks. For instance, P12 shared that their children loved to press a button on a smart switch that controlled lamps, so they *"put a physical barrier up"* to prevent children's access. Several parents mentioned they would keep devices out of their children's reach. Specifically, P8 mentioned that they were afraid that some smart devices could be pushed over and fall on the child. P6 kept smart buttons away from their seven-year-old so the child could not knock the buttons off, which then might pose chocking hazards to the pets. P14 and P22 mentioned efforts to manage device cables, such as ensuring that *"the chords are all hidden"* and *"wrapped up"* so that their children were less likely to accidentally grab the cable and be hit on the head by a falling device. P12 described trying to keep smart speakers out of their youngest one's reach, while acknowledging that such attempts were not always successful:

> *"He presses all the buttons on [the smart speaker] and somehow turns it into like setup mode or turns [the volume] up . . . So we try to keep it out of his reach, but sometimes he climbs to get to things, or he'll pull it down. But we do keep it out of his reach."*

Being selective of children's access to certain devices or functionalities. Zeng and Roesner [109] found that while parents wanted to encourage children's participation in the smart home experiences, they used parental control features to keep their children from causing trouble. We similarly found that parents in our study used additional strategies to limit their children's access to smart home devices or functionalities. Some parents would not register their children's voice with the smart speaker so that the children could not control safety-critical devices such as garage doors and security systems. For instance, P14 described that they opted for *"behind-the-scenes"* voice control restrictions to make the home environment safe instead of explicitly telling children what to do and what not to do:

> *"They can't unlock the door [via voice control]. They can't look at the doorbell. They can't call anyone [via the smart speaker], unless their voices are recognized as . . . an approved user, which they're not . . . I prefer to go with making the system fit them rather than changing their behavior or setting rules in place for them to fit the system."*

Similarly, P23 registered their children's voice to lock the door but did not give the children the code to unlock it. P7 shared that the tablets their children used for watching videos were not integrated into the smart home system, and did not have apps to control other smart home devices.

Safety by obscurity. Several parents mentioned that unless the smart home controls were directly linked to children's activities or experiences, they chose not to tell children how certain controls work, e.g., for thermostats and lights in other family members' room. However, these parents indicated that their children could technically tap on the smart speaker display and use the central app (e.g., Google Home app) to control other smart home devices, because the central app did not allow selective device controls for different users. Due to this limitation, parents developed a "safety by obscurity" mindset and tried to avoid safety issues through intentional non-disclosure. As P20 explained:

> *"If [the kid] knew he could control [the thermostats] . . . there's no way to prevent him from doing it. So I just haven't told him about that stuff . . . and [other] kinds of things that I wouldn't want him to be able to play with . . . like the garage door [and other] security related items."*

Children's age also factored into parents' decision to limit access. P17, with a three- and a six-year-old, said limiting the young children's access to the thermostat was necessary:

> *"They're too young at this point to have access to those sorts of things because of the friction . . . I don't want them to make my AC cost rise . . . I do think it's a little bit more complex and nuanced. It would just take a lot longer for them to figure out."*

Using the device's built-in parental control features. To protect children's digital safety when children use smart speakers to ask questions and browse digital content, nearly all parents mentioned using parental control features to reduce their children's potential exposure to inappropriate content. P10 shared that their children used smart speakers a lot for media consumption and they set up restrictions accordingly:

> *"For the Google Hub: the videos are all set to preteens, the music is all set to non-explicit lyrics . . . [For YouTube apps] we monitor what they watch and also go through the history of what they watch . . . Just make sure . . . those channels are age-appropriate."*

Parents also appropriated other device features as parental controls. For instance, P17 set passwords for smartphones and tablets to prevent their children from accidentally controlling other smart home devices. P14 and P22 configured *"device downtime"* for their smart speakers so that their children could not play music or videos after bedtime.

4.2.3 Parents' rules and guidance for safe use. In addition to putting restrictions in place, many parents established rules and boundaries for appropriate use, provided guidance on dealing with unexpected situations, and instructed their children not to abuse given access.

Rules and boundaries of appropriate use. Most parents shared that they taught children how to appropriately use smart home devices after the initial setup, such as *"what [their children] should and should not do"* in P6's words. Over time, parents gradually established boundaries and rules as children became more familiar with smart home technologies, and parents spent efforts in teaching children how to give commands and exercise controls. As P5 shared:

> *"It took long before they figured out what those rules were, and now I don't really seem to have a problem with them . . . If I add anything to the house, [there] needs to have a rule you can or you can't do this. [The device] is a little bit tempting [to the kids] at first. It quickly loses its attraction . . . Now we understand the rules and that's just how we use it."*

Several parents emphasized the importance of providing reasons behind the rules. P13 gave an example of how they explained their rules for a smart lock:

> *"We try to explain why we don't want him to do stuff. It's not just, 'hey, no, don't do this.' It's 'we don't want you to unlock it, because we don't want the door unlocked [and] we don't want people to come inside.'"*

Education on when things go wrong. When uncertain or unfamiliar events occurred, some parents also taught their children how to react to such situations. P12 said their children were trained to stop the smart speaker if it plays a song that nobody knows as a mechanism to prevent exposure to inappropriate content. P6 highlighted that their child *"knows not to order anything. He knows that if* *the Echo asks him to confirm something, he has to get one of us."* For devices like smart locks and smart speakers, parents shared that their children might keep pressing buttons or failed at getting voice commands executed because of the delayed feedback, and this was a moment when parents would provide guidance. As P11 shared:

> *"There's not a lot of [places] where I forbid them to do something, but I will coach them. With the lock, a lot of times I would say 'It's not going to work if you keep pressing it. You leave it alone, you press it once, and then you wait to see what happens.' "*

Similarly, P23 talked about helping their children when they could not get voice commands to work on the smart speaker:

> *"Sometimes they struggle [with] getting the voice commands right or enunciating properly ... Then I teach them or remind them there's a manual way to do it, or coach them on how to interact with it ... the specific kind of commands to give it or whatnot."*

Regarding smart speakers in particular, similar to what Beneteau et al. [8] have found, parents considered it important to cultivate their children's manners by teaching them to be polite with the speaker in giving voice commands. Sometimes smart speakers can become a conversation disruptor [8] and children become over-reliant on them, so parents might impose more limits, as P4 described:

> *"We'd be having a conversation during dinner, and they're asking [Alexa] a question rather than us. Then she's not getting it right, and she's going on ... It's just annoying. So, we've made a rule now that you can't talk to [Alexa] during dinner, and now they generally know [that] I think that is annoying [and] she can't be part of the conversation."*

Balancing trust and restrictions. Less commonly, parents with older children gave their children unlimited access to and control over smart home devices because they thought their children had proven to be trustworthy rule followers. Nonetheless, parents would still teach children not to abuse or take advantage of the access. For instance, P20 said their nine-year-old *"could go and control everything"* but *"if he abuses it, it's going to [be] taken away."* Such level of trust was typically cultivated through the children's persistent rule-following habits, as P15 explained:

> *"We do a lot of talking to our kids from an early age ... We explain to them and ask them to repeat back and [we] would say 'do you understand why we feel this way, why you can't do this?' They're kind of rule followers, not because we're strict, but because they understand."*

Some children might treat smart home devices as toys. For instance, P22 found that their children were mixing up iPad with Google Home Hub because they both had a touchscreen and could be used for entertainment, so they stressed to the children that Google Home Hub was *"for interacting with the home, not for media consumption."* P17 tried to build conversations around the distinction with their children and called out specific devices that should not be messed with:

> *"Thinking about smart lights, we don't want [kids] turning them on at certain times of the night or playing with them. They're not toys ... along with the security cameras and the doorbell."*

Rules around physical safety. Smart doorbells, and locks were central in conversations around physical safety. Some parents instructed their children to be careful with the smart lock code, and to use the smart doorbell as an alternative to answer the door. For example, P2 granted their children an individual door lock access code but emphasized related rules, such as not sharing the code with anyone else and remembering to re-lock the door if nobody's at home. P4 and P10 both shared experiences of teaching their children to use the smart doorbell safely in line with common home safety rules. As P10 described:

> *"For the video doorbell, unless they know the person we tell them not to talk to anyone. If they don't know the person, then either come get me or my wife or my mom. But we tell them not to talk to strangers [through the video doorbell]."*

P4 added that it took their children practice to understand why it would be safer to check the doorbell display rather than run to the door directly:

> *"For a long time they would run to the door and fling it [open]. We were like, 'come on guys,' because sometimes it's somebody selling something . . . and you don't feel like talking to them. So it took a while for us to train them. They finally did learn . . . So [now] if somebody rang the doorbell, they could just run into the kitchen [to check the doorbell notification on the smart speaker], which you can't see from our front door, and they can see who's there."*

Rules around digital safety. For digital safety, only a few parents said they had taught children what to look out for when using smart home technologies. With security cameras, P22 mentioned that they taught their children to unplug the camera if *"someone yells out [through the camera] and scares them."* P18 discussed with their children about advertisements on Google Home Hub that *"try to sell them things"* and the importance of staying vigilant against these ads. P20 explained to their child that scams and hacking attacks can also occur with smart home devices, hoping that the child could be careful about any solicitations of personal information:

> *"We educated him about scams . . . [If] somebody's email is asking for your information, don't give it to them . . . I feel like the smart home devices kind of open up that same level of risk, like if your Google screen asks you for some information about yourself, you need to question that . . . Why does it want that? . . . It's really just about protecting your information and identity . . . and not giving out information without first questioning it."*

P7 highlighted that maintaining a safe smart home environment and having conversations about different aspects of safety had been a constant effort to them:

> *"I am very careful with them about what they share online, who they can talk to online, and what information they're putting out into the world. Now I say [to my children that] within our home you're always safe, but I also reiterate how the choices that I'm making in our home keeps them that way. Safety is not a one-time event, it is a constant effort . . . We do a lot of . . . talk about what things around the house should you be touching and playing with."*

In summary, in phase 2 parents constantly re-evaluated whether the smart home environment is safe for children and how it could be made safer — safety risks arose as children had limited risk perceptions, were exposed to inappropriate content, or struggled to control the device properly. Parents took measures to mitigate safety risks, such as by removing or limiting access, setting rules, and providing guidance and explanations about risks and for their rules.

4.3 Phase Three: Evolving Safety Needs As Children Grow Up

Beyond immediate safety considerations and mitigation, parents considered how their approaches to safety issues would need to evolve as their children become preteens and teenagers. In contrast to the reactive nature of phase 2, parents described proactively anticipating potential safety risks and needs in the future, such as teaching their children to identify and handle digital safety risks. Parents with young children also foresaw that the children would be more involved in the smart home experience, have their own devices, and eventually demand more privacy and autonomy from their parents.

4.3.1 Need to teach digital safety. Most parents said that they had been closely monitoring their younger children's smart home interactions, so the chances of their children being exposed to risky situations were low at the moment. This explains why only a few parents had discussed digital safety threats with their children directly, but many indicated the necessity of such conversations in the future. As acknowledged by P12: *"we haven't had in-depth educational lessons on privacy and information security . . . [But as] they get more uncontrolled access, we'll have to have more of those conversations."* Several parents further noted that engaging children in digital safety conversations should be done sooner rather than later to help children form safe online habits early on so the lessons will be *"ingrained longer"* (P6) and become critical to cultivate children's *"online hygiene, promoting a learning experience, rather than trying to necessarily [use parental controls to] filter all this [unsafe content] stuff out"* (P13).

4.3.2 Need to adapt parental rules. Parents noted that their current parental rules and mitigation strategies might not work well as their young children become preteens and teenagers. P5 speculated that their children might *"become more independent or a little braver about breaking the rules"* in the next few years, which would require reinforcement of established safety rules. Ur et al. [89] found that teens in their study were uncomfortable with parents' surveillance through auditable door locks and entryway cameras. Similarly, some parents in our study considered making adjustments in reaction to children's potential objection to parental controls when they grow up, as P14 shared:

> *"The [parental controls] that are in place limit what they can do . . . [and] I need them right now. I'm sure once [the children] get older they'll complain, but we'll deal with that as we come to it."*

Some parents anticipated that their children would want to have their own smart home devices and use them in a private setting such as their bedrooms once they grow older. P11 described being aware of the preparation and education needed for such transition. Nevertheless, the quotes from both P11 and P14 conveyed the sentiment that the adaptation of parental rules was something to be addressed later on, and they did not seem to have developed concrete strategies:

> *"If the kids got the Alexa speakers in their rooms . . . especially as they get older and they can start asking it inappropriate questions or adult questions . . . Those are the sort of concerns that I would have as they get older, and if they were to get a more private usage of [the smart devices]. It'll come and I'll have to put a lot of thought into it at that point"* (P11).

4.3.3 Need to build trust. Parents highlighted that a key element in adapting parental rules was to build a trusting relationship with their children and respect the children's autonomy. Both P4 and P13 highlighted that a trusting relationship would foster open parent-child communication. As P4 explained: *"I don't love the idea of censoring them [to ensure their digital safety]. I would much rather be talking to them about all the things that you can find on the Internet."* Similarly, P13 mentioned that when their children have *"questionable questions"* they would turn to the parents first, not the smart speaker. P13 also noted that all the voice commands from the children went to the parents' Amazon account for now, but that would likely change:

> *"When you're starting to talk about them getting to their teenage years, to me . . . it's a conversation of 'should you have your own Amazon account? I'm not your guard anymore because you may want to start asking questions that you don't necessarily feel comfortable sharing with us for whatever reason.' "*

Similarly, P1 and P7 noted that parents need to *"let go of the full control"* at some point. P1 explained that "letting go" means a higher likelihood for children to encounter safety risks, but also more teaching opportunities for parents. P7 highlighted that a precursor to giving children more autonomy is to *"instill natural skepticism:"*

> *"I can't control what they're going to download when they're 13, I'm going to have to let go. The only thing I can do is for the next five years until they turn 13 . . . instill in them this sort of natural skepticism . . . [such as] 'if the product is free, you're the product' . . . I really liked the skepticism that's involved in that thought . . . I have to let go and say I've done the best that I can."*

In summary, phase 3 shows parents' intentions to educate children about digital safety risks and corresponding protective strategies as they grow up. Parents were aware of the need to adapt parental rules in respect of children's autonomy, although they tended to delay thinking about how to do that until a later point. However, not all parents shared the same sentiment toward children's smart home safety, and parental controls in existing smart home technologies might not cater to parents' and children's evolving needs, as we discuss below.

4.4 Factors Influencing Parents' Considerations of Smart Home Child Safety Risks

Across the three phases, we observed that parents' perceptions and approaches regarding smart home child safety were shaped by six factors: parenting style, parents' tech-savviness, parents' trust in tech companies, children's age and developmental differences, news media, and device characteristics.

4.4.1 Parenting style. Among the parents we interviewed, we identified two general parenting styles — vigilant or complacent — in dealing with smart home child safety risks. This dichotomy is in line with the preventative vs. reactive parental approaches in guiding teens to manage privacy risks on social media [101] and the instructive vs. restrictive mediation strategies highlighted in the EU Kids Online network report [54]. Most parents leaned toward the vigilant end in managing perceived safety risks to their children. These parents were aware of and cautious about digital safety risks. Many of them were tech-savvy enough to understand what could go wrong with smart home technologies, and most of them realized how these technologies lacked design considerations for children, which may have contributed to more restrictive and controlling parenting approaches. As such, they tended to be critical in selecting smart home devices and reflected on how their children's privacy and security might be affected.

Vigilant parents with younger children tended to watch out for physical safety risks by deliberately avoiding devices with heat or mechanical components and childproofing smart home technologies to avoid injuries. They also used preventative mediation approaches such as setting rules about smart device use and leveraged existing parental controls [54]. Additionally, many of them considered instructive mediation approaches to educate children about digital smart home safety particularly as the children grow up. For instance, P14 believed that *"in terms of online safety and their privacy [when using smart home technologies] . . . I don't see any problems that can't be solved with education."*

A few parents exhibited a more complacent, relaxed, and trusting sentiment toward children's smart home safety. They appeared to be more optimistic about smart home technologies and emphasized the technologies' benefits over safety risks or privacy implications. Part of the relaxed attitude stems from them being confident that the careful thoughts they put into smart home device selection and management could ensure a safe experience for their children. P13 described encouraging their four-year-old to explore smart home technologies in a guided environment:

> *"I would rather have him have a leg up on [online safety awareness] and have the ability to self regulate screen time and stuff like that at a young age ... as opposed to making [technologies] a forbidden fruit or something that's mysterious and that they have to go somewhere else to learn about."*

4.4.2 Parents' tech-savviness. Many parents described themselves being tech-savvy either because of their occupation or because they were smart home enthusiasts. These parents tended to be intuitively attentive to digital safety, privacy, and security aspects in deciding what devices to purchase, as P8 described *"I'm a safety engineer, so I am already hypersensitive to safety things [about smart home technologies]."* They deliberately avoided certain cloud-based smart devices, such as smart video cameras. Furthermore, some parents weaved their tech-savviness into preventative measures by configuring their home automation from the ground up, paying attention to device updates, and reading privacy policies. P7 gave an example:

> *"I don't use anything that requires a cloud. So that's a total non starter for me. Beyond that, I am probably one of the nine people in the world that actually read the privacy policies and make decisions based on what I read in the privacy policies."*

By contrast, several parents who were not tech professionals did not seem to intuitively associate children's use of smart home technologies with physical safety or security risks. They reflected on how smart home technologies could introduce digital safety risks to children once we probed them about it — some commented that the interview helped them better think about children's smart home safety as they turn to teenagers. As P4 said:

> *"I haven't really thought about this [smart home safety] before our conversation because our kids are very trustworthy ... The idea of them trying to see something that they're not supposed to is not on their radar yet. Now that I think about it, I guess they could be like, 'Hey [Alexa], show me naked pictures.' Yet, I don't think that they're there yet."*

4.4.3 Parents' (dis)trust in tech companies. Similar to Lau et al.'s finding [51] that users' trust toward tech companies plays a critical role in smart speaker adoption, we observed in our study that such trust shaped parents' selection of smart home technologies and which devices they considered safe for their children to use. Many parents indicated that their trust in certain tech companies prompted them to adopt smart home products from the company. For instance, several parents mentioned choosing only HomeKit-compatible [97] smart home products because they trusted Apple exclusively. Others preferred the Google Home system and felt comfortable with their children using Google's products.

On the contrary, some parents expressed distrust toward certain tech companies and thought their products could pose threats to children's digital safety and privacy. These parents tended to avoid purchasing products from distrusted companies or used the product with caution and skepticism. For example, P5 opted for Apple's HomeKit smart home system because they felt annoyed by the business models of companies like Amazon and Google who *"collect information in the market in any way they can."* P14, who was already using the Google Home system, was also upset about Google's lack of transparency in collecting and using their children's data.

4.4.4 Children's age and developmental differences. Not surprisingly, children's age also played an important role in parents' smart home safety considerations. Parents with younger children (i.e., 5-8 years old or younger) considered that their children had a limited understanding of smart home technologies and were not heavily involved in the smart home experience. Consequently, these parents primarily focused on ensuring children's physical safety through child-proofing, such as by putting devices out of children's reach and hiding cables. While many parents would teach young children basic rules (e.g., dos and don'ts about using the smart door lock), some considered digital safety topics too advanced for young children due to their limited online experiences and potential struggles to understand common home safety concepts.

For older children (i.e., ages 8-11, close to preteen years), their parents appeared to worry more about digital safety given older children's wider access to different devices, and these parents described plans to teach their children about digital safety guidelines going forward. Thinking about their children turning into teenagers in a few years, these parents also foresaw their children's needs for more autonomy and privacy in using smart home technologies.

In addition to age, two parents mentioned certain smart home experiences could be a double-edged sword for children with developmental differences. P6 shared that their child with sensory sensitivities found the red lights on smart speakers triggering:

> *"If his Alexa isn't working it will give him a red ring. He actually gets really freaked out by that, very scared of it ... It's really bothersome. We're not sure exactly what that is about it. He's got some social issues so we think that might have something to do with it."*

P3 shared an opposite example by describing how traditional door locks were not user-friendly to their autistic child and why they switched to a smart lock to keep the child safe:

> *"[Before the smart lock] he didn't know how to open the door to go outside ... or he did, but he didn't have the strength to twist the deadbolt. Once he figured out how to do it, he would just go outside and I wouldn't know. And he doesn't tell us like when [he goes outside] ... The risk of him leaving in the middle of night or getting outside and running in the street is much higher for us. That's actually like a real concern."*

4.4.5 News media. When discussing privacy and security concerns around smart security cameras and baby monitors, multiple parents referred to news reports about cameras being hacked to threaten children [93]. This case reinforced parents' caution with using security cameras around children, indicating that some parents' objections to cloud-based cameras were heavily shaped by news reports. For instance, P9 commented that *"even though Amazon owns Ring, I don't entirely trust Ring because of some of the [security breaches] they've had."* These parents decided not to purchase smart cameras, avoided brands implicated in news of data breaches, or only used security cameras in public areas at home but not in children's bedrooms. In line with prior work that shows the influence of news coverage on people's security and privacy behaviors [20, 21, 112], parents in our study tended to be cautious about smart home devices and brands that were featured in news negatively, and considered them unsafe or untrustworthy.

4.4.6 Device characteristics. Device characteristics were a salient influencer of parents' purchase decisions (phase 1). Parents took heat, motors, and a lack of certain product certification (e.g., CE or UL certified) as indicators that the device might pose threats to children's physical safety. Meanwhile, parents thought of digital safety risks for devices that could potentially expose the family's sensitive information, such as security cameras and smart speakers with displays. The consideration of device characteristics continued in phase 2 as parents realized additional safety risks when their children become active users. Specifically, parents considered a device unsafe if children could intentionally or accidentally be exposed to inappropriate content or trigger dangerous home automation actions with physical consequences (e.g., accidentally disarming the security system). As P1 explained:

> *"I would never hook our real security system up to the voice control ... Turning the alarm on and off is not something I want them to be able to do ... Security and physical access control would be two things that I would be uncomfortable with the kids having command access to."*

4.5 Desired improvements to support children's smart home safety

As parents discussed their safety concerns, strategies, and thoughts about evolving safety needs, they brought up desired improvements to support children's safe use of smart home technologies. Two topics were particularly prominent: improved parental controls and more accountability from smart home companies.

4.5.1 Fine-grained and context-adaptive access control. Many parents stressed that an ideal smart home experience should allow parents to pick and choose what parts of the system children can control (e.g., by having a dedicated child profile) and the degree of control (e.g., allowing children to adjust the thermostat by only a few degrees within a defined range). P20, whose nine-year-old could control all smart devices at home, said the first step to ensure children's safety was to give parents *"administrative control"* that could exclude children from accessing certain devices that they should not have control over. P10 shared an idea of enabling smart speakers to distinguish a child's voice and automatically switch to the level of access and control catering to an established child profile:

> *"Right now they don't have their own [Google] account . . . Anyone can use [the home app] . . . It'll be good if Google Home could recognize my kids' voices, like 'oh, this is my son, he's nine years old, so this is the content he's more likely to want, or if he requests something, appropriate content will be served' . . . [and] allow me to be the parent of that account and all the different restrictions."*

P8 added the need to separate the smart home interface for adults and for children, so that their children could *"have their own screens or . . . interfaces to work with, where they're not going to control the house."* P17 envisioned that a smart thermostat could *"add a child's account that could only manipulate things by a few degrees or so."* P14 praised Netflix for allowing individual profiles with customized maturity ratings, but noted that this feature was not available in their voice assistant:

> *"On Netflix I can go to a separate profile for the kids and it locks out the stuff they can't watch, so the [child profile] features are there. But when it comes to the voice assistant interaction, which is where the kids do all of their [interactions] . . . it just uses the defaults."*

Smart speakers were commonly adopted by our parents and many reported that their children often asked smart speakers questions or gave commands. P12, who had four children and multiple smart speakers at home, expressed the desire of *"a digest view"* of activity logs from all children and *"notifications around things that look suspicious."*

4.5.2 Transparency and accountability from smart home companies. While some parents relied on smart home devices' built-in parental controls to protect children's safety, some complained that the parental control setup process could have been more upfront and transparent. P14 recounted that they had never received information or notifications about parental settings from Google, even though Google obviously knew there were young children in the household based on the amount of diaper ads received:

> *"The parental settings that I found weren't advertised to me. At no point did Google say 'hey, you have little kids' or 'if you've got little kids here's how to set up the privacy settings.' I had to go and google parental controls . . . I know that Google knows I have young children. The amount of diaper ads I get . . . they know I have a small child in the house. No point did they go, 'Hey, here's how to protect your kids.' Or 'here's how to control your kid's access.' "*

Another source of frustration for P14 was not knowing how their children's data had been collected and used and not being able to delete collected information:

"As a parent, I would like more information on what is known about my kids. I assume somewhere there is 'these kids are really into Frozen and The Little Mermaid and they like to turn the lights on at this time of the morning' ... I know that that profile exists. I would like the transparency [from Google] to say that it exists, and I would like the ability to delete it. I know that in the European Union, they have the ability to ask tech companies to delete profiles, the fact that it doesn't exist in North America, even for the adults is interesting. ... [My kids] are minors [and] they don't have that advocacy to go 'I don't want this.' They can't check on the 'I don't consent' box on websites."

P17, who worked with one of the major smart speaker manufacturers, raised that most smart speakers in the market offered limited parental control options and companies had little incentive to improve this. P17 wanted to involve children more in the smart home experiences, but worried about shady practices around the collection and use of their children's data:

"It's not enough to put the responsibility of safety and security on just the user ... I really love the idea of ... childproofing your smart home. [But] it's in its infancy ... I do a lot of work with [company] and their general stance is that we don't talk about [childproofing] with kids under the age of 13 because they just don't want to take responsibility."

Another reason to increase the accountability of smart home companies is that not all users are able to and empowered to protect their children's online safety. P21 considered themselves not that tech-savvy and worried that their children would soon be able to bypass parental controls, calling for more educational efforts by companies:

"It will be better if [those companies] can have parent tutorials ... I feel like ... if you're not tech savvy, then it's hard for you to get on top of everything ... I like it's easier on this age [when children are young], but they grow [more tech-savvy] and they will get better [at breaking parental rules]."

P6 drew from their occupation as a technical writer in discussing how companies should educate users. Emami-Naeini et al. [27] proposed privacy and security "nutrition labels" for IoT devices to inform consumers' purchase decisions. Akin to this idea, P6 envisioned that companies can feature safety-relevant information when there are new updates and on the product's front page saliently:

"As smart devices evolve ... you really need a good system for teaching people how to stay secure on their own devices ... When there are new updates and stuff, [then] people should have to go through a new security tutorial ... I actually think that the primary source of risk mitigation should be through education and the sharing of information ... I think a lot about smart home stuff and the way it's advertised, as [the company] doesn't tell you the drawbacks of them ... I just don't think they're putting [risks] on the main page [to inform the users]."

The main takeaway is that parents should not be solely responsible for children's smart home safety. Instead, more systematic effort is required to ensure smart home technologies provide safe and child-centered digital experiences [77]. Our findings indicate that parents rely on parental control features in smart home devices to manage children's safe use, demand more transparency on how children's data is collected/used, and desire educational resources to support both parents and children in protecting themselves from smart home safety risks.

5 DISCUSSION

Our findings contribute insights on parents' perception of smart home child safety risks across three phases, factors that influence parents' safety perceptions, and parents' strategies to mitigate perceived safety risks. Next, we discuss our findings in relation to prior work and conclude with our study's implications for designers and policymakers to better support child safety in smart homes.

5.1 Child Safety Risks in Smart Homes Are Nuanced

Prior work has examined children's physical home safety [44, 52, 64] and online digital safety needs [54–56] in relation to parents' involvement. Building on this, our study investigated parents' perceptions of children's safety in interacting with smart home technologies. Our findings highlight that parents' perceptions of child safety risks in smart homes are nuanced, include both physical and digital aspects, and evolve across different phases.

5.1.1 Evolving smart home safety needs. In examining parents' considerations of child safety risks in smart homes, it is worth noting that child safety had already been factored into parents pre-purchase considerations and decisions. Parents were cautious about devices that might pose obvious physical safety, privacy, or security risks. However, even though parents thought about safety, many safety risks did not emerge until children started interacting with the smart devices at home. Examples of unanticipated safety risks included physical safety incidents due to children's inappropriate use and exposure to unsuitable content due to the ease with which children could often access multiple devices in a connected home, in particular when smart speakers' voice interaction lowered the access barrier for children.

Karapanos et al. [41] highlighted the temporality of user experience: consumers' acceptance and evaluation of products constitute a reflective process across multiple phases from pre-purchase to post-consumption. More specific to smart home technologies, Emami-Naeini et al. [28] found that privacy and security were not primary considerations in consumers' purchase decisions, but became more salient through later use. While parents in our study appeared to be more aware of privacy and security risks before purchase as they actively thought about safety risks for their children, parents' evaluation of children's smart home safety evolved with actual use, prompting them to reactively adapt mitigation strategies to their changing safety risk perceptions. Our findings show that parents have little support in figuring out child safety risks in advance, resulting in unpleasant – and potentially dangerous – surprises during actual use. This indicates a need for better support mechanisms that help parents comprehensively consider child safety risks in pre-purchase evaluation.

Furthermore, our findings suggest that parents recognize the need to adapt parental rules as children grow up (phase 3), such as by shifting the focus on education about digital safety and giving children more agency in accessing and using smart home devices. These findings echo prior work on parent-teen interactions regarding online safety risks [10, 18, 29, 100, 101], which has highlighted that teenagers desire some degree of privacy and autonomy from their parents in navigating the online world. Nevertheless, parents in our study tended to defer the development of concrete strategies to the future. The lack of granular parental controls in smart home technologies further casts doubt on whether parents can find a middle ground between having no or too restrictive controls in place. Too passive interventions or no intervention may amplify children's exposure to risks, whereas too paternalistic approaches may diminish interpersonal trust [18] and reduce opportunities for children to learn about effective risk-coping [101].

5.1.2 Smart home amplifies conventional physical and digital child safety risks. Prior research has primarily studied privacy and security issues in family use of smart home technologies, with children often framed as smart home passive users or bystanders [46, 51, 106–108]. Other work has examined online safety risks [54, 57] and physical home safety issues [44, 81] related to children. Our findings highlight that smart home technologies deserve particular attention as they combine both physical and digital safety risks for children. On one hand, smart home technologies are physical objects, which are comparable to more traditional household appliances in terms of their capability of introducing safety hazards, particularly for children who are usually adventurous experimenters and unconventional users. On the other hand, smart home technologies serve as portals to the Internet and varying digital experiences; such connections open the door to complex information flows, child-inappropriate content, or even surveillance and harassment from strangers when the device is compromised.

Our findings show that some parents used conventional child-proofing techniques on smart home devices such as organizing cables to avoid strangulation, keeping devices out of children's reach to prevent injuries, and hiding small devices that pose choking hazards. Parents' child-proofing efforts for smart home devices were similar to how parents would child proof other objects in their home. Nonetheless, even with child-proofing efforts, parents still reported unanticipated safety incidents such as a smart vacuum accidentally running over children's toes and knocking items down. Such incidents provide evidence that existing smart home devices have not sufficiently considered child safety in hardware design. By contrast, other objects in the home, such as furniture and appliances are either pre-equipped with child safety measures or can be readily augmented to make them child safe. For instance, tall furniture, such as book shelves or dressers, often include retaining straps to mount them to the wall and prevent them from tipping over when a child climbs up on them. Similarly, electrical appliances such as ovens, dishwashers, and washing machines often have child safety locks that can be set to prevent young children from opening their doors. Cabinet doors can be easily augmented with magnetic child safety locks, and stove top controls can be made child-safe with special knobs that prevent activation by children. Comparable safety measures are lacking for most smart home technologies.

Furthermore, smart home technologies amplify existing safety risks for children [86]. Prior research has uncovered gaps in children's mental models of online privacy risks [49, 84, 111]; our study similarly shows that children's awareness and perception of smart home safety risks are limited due to immature cognition and a tendency to treat smart home devices as toys. Enabling the control of many devices and home automation with voice commands substantially lowers barriers for children to trigger a swath of smart home devices including safety-critical ones. For instance, a child could ask the smart speaker to increase the temperature for a connected smart water heater to dangerous levels, or accidentally unlock doors and let strangers into the home using voice commands and without parents' permission. While parents in our study described these situations as hypotheticals, they are realistic and could cause severe consequences. Smart home technologies, particularly smart speakers as the control hub for smart homes, are placed centrally in homes to facilitate ease of interaction [51], further reducing the access barriers compared to a smart home app on a parent's password-protected phone.

Our study shows that parents are gatekeepers who identify and ensure children's evolving safety needs in the smart home environment. However, the lack of child-centered design considerations in smart home technologies amplifies conventional physical and digital child safety risks. Examples of home appliances with child safety measures suggest that enjoying the benefits of smart home technologies and ensuring child safety do not have to be a trade-off; one can have both as long as smart home technologies adopt child-centered design — design that acknowledges and empowers children's need for safety and autonomy [77].

5.2 Design and Policy Implications

Drawing from our findings, we discuss how smart home product design should reduce child safety risks through providing child-centered smart home experiences by default and more granular parental controls for risk management. We further note the need for more transparency and educational efforts from smart home companies.

5.2.1 Child-Safety-Centered Design in Smart Home Technologies. We argue that smart home technologies targeted for family use should incorporate child-safety design features, as our findings reveal that smart home technologies could pose physical and digital safety risks when they are placed in the home environment and used by children in unconventional or unintended ways. Making smart home technologies safer for children does not necessarily sacrifice the product experience, as shown in many other products for which child safety is an important design consideration or built-in feature due to regulatory requirements. For instance, the US Consumer Product Safety Commission requires that all child-facing products (consumer products designed or intended primarily for children 12 years old or younger) comply with a set of federal safety rules, e.g., the product should avoid restricted substances and sharp points or edges [15]. Even for products that are not specifically designed for children but could be in frequent contact with children, many have incorporated child safety measures [15]. Containers, washing machines, and many other home appliances have conventional child safety locks to prevent children from reaching dangerous contents, randomly pressing buttons, or engaging in risky behaviors. Robomow, a smart lawnmower, has child locks and automatic stop features to protect children from getting hurt when it detects obstacles [95].

The concept of *optimal defaults* describes how environmental design that makes default decisions the healthiest can positively impact human flourishing [32]. Similarly, *child-centered defaults* [77] consider children's well-being as a priority by changing the environmental and structural determinants rather than delegating gate-keeping responsibilities to parents and caregivers. Drawing inspirations from these concepts, we advocate that smart home tech companies should adopt a *child-safety-centered design* approach by rethinking how child safety needs should factor into the product design as a first principle. Child-centered experiences [77] with appropriate safety measures and interventions can be established through available user settings and choice architecture [85]. As an example, smart robot vacuums are not intended for children's use but could be in an environment that involves children. A child-safety-centered design approach could involve ongoing testing of smart home devices for the unexpected ways that children may use them (e.g., for smart robot vacuums, have sensors that detect children's presence and weight, as some children like to step on the vacuum [34]). Exploratory work with parents could examine what types of safety settings could decrease chances of accidents (e.g., a confirmation step before vacuum activation that asks "Are you sure there are no children in this area?"). For all smart home technologies that are advertised for family use, smart home companies should further conduct evidence-based safety testing to understand how children might be in contact with, use, or potentially abuse the device in order to reduce the possibility of safety issues as part of the product design.

5.2.2 Granular Parental Controls. Smart home technologies have been found to create tensions among different user groups such as couples, roommates, and parents and children/teenagers due to their different levels of access, power, and needs [26, 33, 46, 51, 89, 109]. Similarly, parents in our study unanimously complained about the lack of customization and granularity in existing parental control features, which suggests that current smart home technology design lacks the consideration of multi-user scenarios. While prior work has noted that children are becoming active smart home users and should be considered in technology design [79], our findings show that most smart home products do not yet seem to recognize children as a critical audience with unique usage patterns and needs. Safety issues arise as children have a limited understanding of both how smart home technologies work and potential safety risks. Moreover, our findings suggest that some children are prone to treating smart home technologies as toys; others might accidentally trigger actions by pressing buttons or through voice commands. Some parents specifically commented on tech companies' insufficient efforts in considering, communicating, and implementing child safety features.

Our findings align with prior work [18, 33, 36, 39, 108, 109] in identifying that the "all or nothing" access control fails in family settings when children and teenagers are treated as passive users. Without meaningful parental controls, parents were struggling with managing child safety issues, and some expressed desires for more selective access management as part of parental controls. Rather than allowing children to control all devices in the home, parents wanted to give children control only over certain devices (e.g., smart lights in the child's bedroom) while restricting access to others (e.g., lights in a sibling's bedroom) and preventing access to safety-critical devices (e.g., security systems and smart water heaters). Several parents brought up the idea of a child profile for smart home systems that would provide limited, child-friendly, and safe access to parts of the smart home. Considering children's unique usage patterns and experiences in product design would be an important step toward making space for children in the family [17, 75] — children are and should be viewed as equal members of the family, and this ideology should be reflected in product design. Children should be able to actively participate in the smart home environment in ways that ensure their safety, promote their sense of autonomy and competency, and enable adaptation over time. Policymakers and regulators should urge or require companies to provide granular and context-adaptive controls that are easier to use and more helpful for parents to limit what their children can access.

5.2.3 Accountability And Transparency to Support Children's Safety. Several parents highlighted that smart home companies should be held accountable for being transparent about data practices and for supporting parents to protect children's safety in smart homes. P14's shared experience with Google provides a vivid example: their children's daily interactions with Google Home had enabled Google to make inferences about the family status and send diaper ads regularly; however, they felt Google had never been transparent about what and how their children's data was collected and used, nor did the company attempt to use the respective inferences to make the parents aware of options to manage child safety or delete the collected data.

Smart home devices intended for family use capture a wealth of data — including children's data — inevitably or even intentionally. Current privacy laws such as the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA) and the Children's Online Privacy Protection Act (COPPA) in the US require companies to obtain parental consent for processing of their children's data. Nevertheless, smart home companies rarely incorporate parental consent or offer options to limit data collection about children because the devices are targeted at adults – conveniently ignoring the fact that they are frequently placed in family settings and used by children of all ages. The large amount of data companies are collecting and making inferences from should be used to help parents better protect their children instead of generating targeted ads as the primary or even sole purpose. In all, companies should be held accountable to make smart home technologies safer for children and family, rather than pretending "there are no users under the age of 13" to avoid liabilities.

5.2.4 Support Parents With Educational Efforts. Many parents in our study were tech-savvy, likely because we recruited parents who were already smart home adopters. However, existing research shows that most adults do not have a clear understanding of data collection, profiling, and relevant data protection laws in smart homes and other contexts [5, 40, 76, 109]; low-income parents in particular struggle to properly support children's tech use and keep up with the latest changes in technologies [78]. As several parents in our study highlighted, tech companies should put more effort into educating parents (and users in general) about privacy, security, and safety aspects of their products. Doing this would empower parents to be more informed when deciding to adopt products and more resourceful when it comes to teaching and protecting children in using smart home technologies.

We argue that tutorials and resources about safety should be a default part of the on-boarding experience and throughout updates for smart home technologies. For child-facing and child-involving smart home products, smart home companies should ideally be required to provide guidance and resources on child safety as part of the parental control settings to demonstrate the company's commitment to children's safety. Prior work has proposed "privacy nutrition labels" as an improved format of traditional privacy policies to better communicate companies' data practices [42, 43], and this idea has led to Apple's privacy labels for mobile apps in iOS 14 [12]. Emami-Naeini et al. [27] proposed privacy and security labels for IoT devices, including ratings from independent privacy assessment organizations, data collection types, and scenarios.

Following a child-safety-centered design approach, we see the potential of incorporating child safety information into smart home device labels to communicate safety ratings, appropriate age for children's use, and different types of potential safety risks to children. Such information could alleviate parents' gate-keeping burden and help parents better evaluate child safety risks in making purchase decisions, instead of having parents caught by surprise once safety issues arise during children's smart home use. Moreover, federal regulatory agencies such as the US Consumer Product Safety Commission [15] should prescribe standards for the form and content of child safety labels for smart home devices and oversee corresponding evidence-based research and design.

6 CONCLUSION

Through 23 semi-structured interviews with parents who are smart home technology adopters, we uncovered that parents' perceptions of and mitigation strategies for child safety in smart homes covered both physical and digital aspects and evolved through three phases: considerations before purchase decisions, re-evaluation of safety risks during use, and adaptation to changing safety needs as children grow up. We identified six factors that shaped parents' safety perceptions and mitigation strategies, including parenting style, parents' tech-savviness, parents' trust in tech companies, children's age and developmental differences, news media, and device characteristics. Our findings indicate opportunities for smart home products to incorporate child safety features and provide more granular parental controls. Furthermore, smart home companies should acknowledge that many of their products are child-facing or child-involving. As such, companies should take responsibility and be held accountable for properly considering and mitigating child safety risks in product design.

ACKNOWLEDGMENTS

This research has been partially funded by a University of Michigan MCubed grant (#9138) and by the University of Michigan School of Information. We thank Amelia Smith and Maxwell Rosenzweig for their research assistance. We are also grateful to all the participating families and the anonymous reviewers for their constructive feedback.

REFERENCES

[1] Frances K Aldrich. 2003. Smart homes: past, present and future. In *Inside the smart home*. Springer, UK, 17–39. https://doi.org/10.1007/1-85233-854-7_2

[2] Tawfiq Ammari, Sarita Schoenebeck, and Daniel Romero. 2019. Self-declared throwaway accounts on Reddit: How platform affordances and shared norms enable parenting disclosure and support. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 135:1–135:30. https://doi.org/10.1145/3359237

[3] Tawfiq Ammari, Sarita Schoenebeck, and Daniel M Romero. 2018. Pseudonymous parents: Comparing parenting roles and identities on the Mommit and Daddit subreddits. In *ACM Conference on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, 489:1–489:13. https://doi.org/10.1145/3173574.3174063

[4] Alan R Andreasen. 1977. A taxonomy of consumer satisfaction/dissatisfaction measures. *Journal of Consumer Affairs* 11, 2 (1977), 11–24. https://doi.org/10.1111/j.1745-6606.1977.tb00612.x

[5] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. 2019. *Americans and privacy: Concerned, confused and feeling lack of control over their personal information.* Technical Report. Pew Research Center. https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf

[6] Nazmiye Balta-Ozkan, Rosemary Davidson, Martha Bicket, and Lorraine Whitmarsh. 2013. Social barriers to the adoption of smart homes. *Energy Policy* 63 (2013), 363–374. https://doi.org/10.1016/j.enpol.2013.08.043

[7] Andrea Bellucci, Giulio Jacucci, Veera Kotkavuori, Bariş Serim, Imtiaj Ahmed, and Salu Ylirisku. 2015. Extreme Co-design: Prototyping with and by the User for Appropriation of Web-connected Tags. In *International Symposium on End User Development.* Springer, 109–124. https://doi.org/10.1007/978-3-319-18425-8_8

[8] Erin Beneteau, Ashley Boone, Yuxing Wu, Julie A Kientz, Jason Yip, and Alexis Hiniker. 2020. Parenting with Alexa: exploring the introduction of smart speakers on family dynamics. In *ACM Conference on Human Factors in Computing Systems (CHI).* Association for Computing Machinery, 217:1–217:13. https://doi.org/10.1145/3313831.3376344

[9] Erin Beneteau, Olivia K Richards, Mingrui Zhang, Julie A Kientz, Jason Yip, and Alexis Hiniker. 2019. Communication breakdowns between families and Alexa. In *ACM Conference on Human Factors in Computing Systems (CHI).* Association for Computing Machinery, 243:1–243:13. https://doi.org/10.1145/3290605.3300473

[10] Danah Boyd. 2014. *It's complicated: The social lives of networked teens.* Yale University Press.

[11] J Joško Brakus, Bernd H Schmitt, and Lia Zarantonello. 2009. Brand experience: what is it? How is it measured? Does it affect loyalty? *Journal of Marketing* 73, 3 (2009), 52–68. https://doi.org/10.1509/jmkg.73.3.052

[12] Ian Carlos Campbell. 2020. Apple will require apps to add privacy 'nutrition labels' starting December 8th. https://www.theverge.com/2020/11/5/21551926/apple-privacy-developers-nutrition-labels-app-store-ios-14

[13] Jilin Chen, Gary Hsieh, Jalal U Mahmud, and Jeffrey Nichols. 2014. Understanding individuals' personal values from social media word use. In *ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW).* Association for Computing Machinery, 405–414. https://doi.org/10.1145/2531602.2531608

[14] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N Patel, and Julie A Kientz. 2012. Investigating receptiveness to sensing and inference in the home using sensor proxies. In *ACM Conference on Ubiquitous Computing (UbiComp).* Association for Computing Machinery, 61–70. https://doi.org/10.1145/2370216.2370226

[15] United States Consumer Product Safety Commission. 2021. Children's Products. https://www.cpsc.gov/Business--Manufacturing/Business-Education/childrens-products

[16] Diane J Cook. 2012. How smart is your home? *Science* 335, 6076 (2012), 1579–1581. https://doi.org/10.1126/science.1217640

[17] William A Corsaro. 2017. *The sociology of childhood.* Sage publications.

[18] Lorrie Faith Cranor, Adam L Durity, Abigail Marsh, and Blase Ur. 2014. Parents' and teens' perspectives on privacy in a technology-filled world. In *Symposium On Usable Privacy and Security (SOUPS).* USENIX Association, 19–35. https://www.usenix.org/system/files/conference/soups2014/soups14-paper-cranor.pdf

[19] Sarah Darby. 2010. Smart metering: what potential for householder engagement? *Building research & information* 38, 5 (2010), 442–457. https://doi.org/10.1080/09613218.2010.492660

[20] Sauvik Das, Laura A Dabbish, and Jason I Hong. 2019. A typology of perceived triggers for end-user security and privacy behaviors. In *Symposium on Usable Privacy and Security (SOUPS).* USENIX Association, 97–115. https://www.usenix.org/system/files/soups2019-das.pdf

[21] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I Hong. 2018. Breaking! A Typology of Security and Privacy News and How It's Shared. In *ACM Conference on Human Factors in Computing Systems (CHI).* Association for Computing Machinery, 1:1–1:12. https://doi.org/10.1145/3173574.3173575

[22] Scott Davidoff, Min Kyung Lee, Charles Yiu, John Zimmerman, and Anind K Dey. 2006. Principles of smart home control. In *ACM International Conference on Ubiquitous Computing (UbiComp).* Association for Computing Machinery, 19–34. https://doi.org/10.1007/11853565_2

[23] J Delgado, ME Ramirez-Cardich, Robert H Gilman, R Lavarello, N Dahodwala, A Bazan, V Rodriguez, RI Cama, M Tovar, and A Lescano. 2002. Risk factors for burns in children: crowding, poverty, and poor maternal education. *Injury Prevention* 8, 1 (2002), 38–41. https://doi.org/10.1136/ip.8.1.38

[24] Tamara Denning, Tadayoshi Kohno, and Henry M Levy. 2013. Computer security and the modern home. *Commun. ACM* 56, 1 (2013), 94–103. https://doi.org/10.1145/2398356.2398377

[25] Robert A Dershewitz and Edward R Christophersen. 1984. Childhood household safety: An overview. *American Journal of Diseases of Children* 138, 1 (1984), 85–88. https://doi.org/10.1001/archpedi.1984.02140390073022

[26] Nils Ehrenberg and Turkka Keinonen. 2021. The Technology Is Enemy for Me at the Moment: How Smart Home Technologies Assert Control Beyond Intent. In *ACM Conference on Human Factors in Computing Systems (CHI).* Association for Computing Machinery, 407:1–407:11. https://doi.org/10.1145/3411764.3445058

[27] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the Experts: What Should Be on an IoT Privacy and Security Label?. In *Symposium on Security and Privacy*. IEEE, 447–464. https://doi.org/10.1109/SP40000.2020.0004

[28] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring how privacy and security factor into IoT device purchase behavior. In *ACM Conference on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, 534:1–534:12. https://doi.org/10.1145/3290605.3300764

[29] Lee B Erickson, Pamela Wisniewski, Heng Xu, John M Carroll, Mary Beth Rosson, and Daniel F Perkins. 2016. The boundaries between: Parental involvement in a teen's online world. *Journal of the Association for Information Science and Technology* 67, 6 (2016), 1384–1403. https://doi.org/10.1002/asi.23450

[30] Robert J Fisher. 1993. Social desirability bias and the validity of indirect questioning. *Journal of Consumer Research* 20, 2 (1993), 303–315. https://doi.org/10.1086/209351

[31] Internet Safety Technical Task Force. 2009. *Enhancing Child Safety and Online Technologies*. Technical Report. The Berkman Center for Internet & Society, Harvard University. https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf

[32] Thomas R Frieden. 2010. A framework for public health action: the health impact pyramid. *American journal of public health* 100, 4 (2010), 590–595.

[33] Christine Geeng and Franziska Roesner. 2019. Who's In Control? Interactions In Multi-User Smart Homes. In *ACM Conference on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, 268:1–268:13. https://doi.org/10.1145/3290605.3300498

[34] Samantha Grossman. 2015. Here's a Cute Baby Riding a Roomba Like a Total Pro. https://time.com/3889326/baby-riding-roomba-video/

[35] Anita Gärling and Tommy Gärling. 1995. Mothers' anticipation and prevention of unintentional injury to young children in the home. *Journal of Pediatric Psychology* 20, 1 (1995), 23–36. https://doi.org/10.1093/jpepsy/20.1.23

[36] Tom Hargreaves, Charlie Wilson, and Richard Hauxwell-Baldwin. 2018. Learning to live in a smart home. *Building Research & Information* 46, 1 (2018), 127–139. https://doi.org/10.1080/09613218.2017.1286882

[37] Patrick CK Hung, Farkhund Iqbal, Shih-Chia Huang, Mohammed Melaisi, and Kevin Pang. 2016. A glance of child's play privacy in smart toys. In *International Conference on Cloud Computing and Security*. Springer, 217–231. https://doi.org/10.1007/978-3-319-48674-1_20

[38] Timo Jakobi, Corinna Ogonowski, Nico Castelli, Gunnar Stevens, and Volker Wulf. 2017. The catch (es) with smart home: Experiences of a living lab field study. In *ACM Conference on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, 1620–1633. https://doi.org/10.1145/3025453.3025799

[39] William Jang, Adil Chhabra, and Aarathi Prasad. 2017. Enabling multi-user controls in smart home devices. In *ACM Workshop on Internet of Things Security and Privacy*. Association for Computing Machinery, 49–54. https://doi.org/10.1145/3139937.3139941

[40] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere": User Mental Models of the Internet and Implications for Privacy and Security. In *Symposium On Usable Privacy and Security (SOUPS)*. USENIX Association, 39–52. https://www.usenix.org/system/files/conference/soups2015/soups15-paper-kang.pdf

[41] Evangelos Karapanos, John Zimmerman, Jodi Forlizzi, and Jean-Bernard Martens. 2009. User experience over time: an initial framework. In *ACM Conference on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, 729–738. https://doi.org/10.1145/1518701.1518814

[42] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W Reeder. 2009. A "nutrition label" for privacy. In *Symposium on Usable Privacy and Security (SOUPS)*. Association for Computing Machinery, 4:1–4:12. https://doi.org/10.1145/1572532.1572538

[43] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. 2010. Standardizing privacy notices: an online study of the nutrition label approach. In *ACM Conference on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, 1573–1582. https://doi.org/10.1145/1753326.1753561

[44] Denise Kendrick, Ben Young, Amanda J Mason-Jones, Nohaid Ilyas, Felix A Achana, Nicola J Cooper, Stephanie J Hubbard, Alex J Sutton, Sherie Smith, Persephone Wynn, et al. 2013. Home safety education and provision of safety equipment for injury prevention. *Evidence-based child health: a Cochrane review journal* 8, 3 (2013), 761–939. https://doi.org/10.1002/ebch.1911

[45] Nikos Komninos, Eleni Philippou, and Andreas Pitsillides. 2014. Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys & Tutorials* 16, 4 (2014), 1933–1954. https://doi.org/10.1109/COMST.2014.2320093

[46] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. 2021. "We Just Use What They Give Us": Understanding Passenger User Perspectives in Smart Homes. In *ACM Conference on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, 41:1–41:14. https://doi.org/10.1145/3411764.3445598

[47] Tiiu Koskela and Kaisa Väänänen-Vainio-Mattila. 2004. Evolution towards smart home environments: empirical evaluation of three user interfaces. *Personal and Ubiquitous Computing* 8, 3-4 (2004), 234–240. https://doi.org/10.1007/s00779-004-0283-x

[48] Jennie Jacobs Kronenfeld, Mark Reiser, Deborah C Glik, Carlos Alatorre, and Kirby Jackson. 1997. Safety behaviors of mothers of young children: Impact of cognitive, stress and background factors. *Health* 1, 2 (1997), 205–225. https://doi.org/10.1177/136345939700100205

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

[50] Frederick S Lane. 2012. *Cybertraps for the Young*. NTI Upstream.

[51] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, are you listening? privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 102:1–102:31. https://doi.org/10.1145/3274371

[52] John C LeBlanc, I Barry Pless, W James King, Harry Bawden, Anne-Claude Bernard-Bonnin, Terry Klassen, and Milton Tenenbein. 2006. Home safety measures and the risk of unintentional injury among young children: a multicentre case–control study. *CMAJ* 175, 8 (2006), 883–887.

[53] Simon CR Lewis. 2011. Energy in the smart home. In *The connected home: The future of domestic life*. Springer, 281–300. https://doi.org/10.1007/978-0-85729-476-0_14

[54] Sonia Livingstone, Leslie Haddon, Anke Görzig, and Kjartan Ólafsson. 2011. *Risks and safety on the internet: The perspective of European children*. Technical Report. EU Kids Online Network. http://eprints.lse.ac.uk/33731/1/Risks%20and%20safety%20on%20the%20internet%28lsero%29.pdf

[55] Sonia Livingstone, Giovanna Mascheroni, Michael Dreier, Stephane Chaudron, and Kaat Lagae. 2015. *How parents of young children manage digital devices at home: The role of income, education and parental style*. Technical Report. http://eprints.lse.ac.uk/63378/

[56] Sonia Livingstone, Kjartan Ólafsson, Ellen J Helsper, Francisco Lupiáñez-Villanueva, Giuseppe A Veltri, and Frans Folkvord. 2017. Maximizing opportunities and minimizing risks for children online: The role of digital skills in emerging strategies of parental mediation. *Journal of Communication* 67, 1 (2017), 82–105. https://doi.org/10.1111/jcom.12277

[57] Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri. 2019. *Children's data and privacy online: growing up in a digital age: an evidence review*. Technical Report. London School of Economics and Political Science. http://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf

[58] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019), 250–271. https://doi.org/10.2478/popets-2019-0068

[59] Adam P Matheny Jr. 1986. Injuries among toddlers: Contributions from child, mother, and family. *Journal of Pediatric Psychology* 11, 2 (1986), 163–176. https://doi.org/10.1093/jpepsy/11.2.163

[60] Christian F Mauro and Yvette R Harris. 2000. The influence of maternal child-rearing attitudes and teaching behaviors on preschoolers' delay of gratification. *The Journal of Genetic Psychology* 161, 3 (2000), 292–306. https://doi.org/10.1080/00221320009596712

[61] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys that listen: A study of parents, children, and internet-connected toys. In *ACM Conference on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, 5197–5207. https://doi.org/10.1145/3025453.3025735

[62] Charles Mock, Carlos Arreola-Risa, Rodolfo Trevino-Perez, Victoria Almazan-Saavedra, Jaime E Zozaya-Paz, Reynaldo Gonzalez-Solis, Kate Simpson, Laura Rodriguez-Romo, and Martin H Hernandez-Torre. 2003. Injury prevention counselling to improve safety practices by parents in Mexico. *Bulletin of the World Health Organization* 81 (2003), 591–598. https://www.scielosp.org/pdf/bwho/2003.v81n8/591-598/en

[63] Barbara A Morrongiello and M Corbett. 2006. The parent supervision attributes profile questionnaire: a measure of supervision relevant to children's risk of unintentional injury. *Injury Prevention* 12, 1 (2006), 19–23. https://doi.org/10.1136/ip.2005.008862

[64] Barbara A Morrongiello, Michael Corbett, Jennifer Lasenby, Natalie Johnston, and Meghan McCourt. 2006. Factors influencing young children's risk of unintentional injury: Parenting style and strategies for teaching about home safety. *Journal of applied developmental psychology* 27, 6 (2006), 560–570.

[65] Barbara A Morrongiello and Sophie Kiriakou. 2004. Mothers' home-safety practices for preventing six types of childhood injuries: what do they do, and why? *Journal of Pediatric Psychology* 29, 4 (2004), 285–297. https://doi.org/10.1093/jpepsy/jsh030

[66] Barbara A Morrongiello, Corina Midgett, and Roslyn Shields. 2001. Don't run with scissors: young children's knowledge of home safety rules. *Journal of Pediatric Psychology* 26, 2 (2001), 105–115. https://doi.org/10.1093/jpepsy/26.2.105

[67] Barbara A Morrongiello, Lisa Ondejko, and Amanda Littlejohn. 2004. Understanding toddlers' in-home injuries: I. Context, correlates, and determinants. *Journal of Pediatric Psychology* 29, 6 (2004), 415–431. https://doi.org/10.1093/jpepsy/jsh046

[68] Soraya Sarhaddi Nelson. 2017. Germany Bans My Friend Cayla Doll Over Spying Concerns. https://www.npr.org/2017/02/20/516292295/germany-bans-my-friend-cayla-doll-over-spying-concerns

[69] Peter Nikken and Marjon Schols. 2015. How and why parents guide the media use of young children. *Journal of Child and Family Studies* 24, 11 (2015), 3423–3435. https://doi.org/10.1007/s10826-015-0144-4

[70] Sang Hyun Park, So Hee Won, Jong Bong Lee, and Sung Woo Kim. 2003. Smart home–digitally engineered domestic life. *Personal and Ubiquitous Computing* 7, 3-4 (2003), 189–196. https://doi.org/10.1007/s00779-003-0228-9

[71] Charith Perera, Ciaran McCormick, Arosha K Bandara, Blaine A Price, and Bashar Nuseibeh. 2016. Privacy-by-design framework for assessing internet of things applications and platforms. In *ACM International Conference on the Internet of Things*. Association for Computing Machinery, 83–92. https://doi.org/10.1145/2991561.2991566

[72] Lizette Peterson, Janet Farmer, and Javad H. Kashani. 1990. Parental injury prevention endeavors: A function of health beliefs? *Health Psychology* 9, 2 (1990), 177–191. https://doi.org/10.1037/0278-6133.9.2.177

[73] Eleni Petridou, Dimitrios Trichopoulos, E Mera, Y Papadatos, K Papazoglou, A Marantos, and C Skondras. 1998. Risk factors for childhood burn injuries: a case-control study from Greece. *Burns* 24, 2 (1998), 123–128. https://doi.org/10.1016/S0305-4179(97)00095-8

[74] Todd Powers, Dorothy Advincula, Manila S Austin, Stacy Graiko, and Jasper Snyder. 2012. Digital and social media in the purchase decision process: A special report from the Advertising Research Foundation. *Journal of Advertising Research* 52, 4 (2012), 479–489. https://doi.org/10.2501/JAR-52-4-479-489

[75] Jens Qvortrup, William A Corsaro, Michael-Sebastian Honig, and Gill Valentine. 2009. *The Palgrave handbook of childhood studies*. Palgrave Macmillan, UK.

[76] Emilee Rader, Samantha Hautea, and Anjali Munasinghe. 2020. "I Have a Narrow Thought Process": Constraints on Explanations Connecting Inferences and Self-Perceptions. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, USA, 457–488. https://www.usenix.org/system/files/soups2020-rader.pdf

[77] Jenny Radesky and Alexis Hiniker. 2021. From moral panic to systemic change: Making child-centered design the default. *International Journal of Child-Computer Interaction* (2021), 100351.

[78] Jenny S Radesky, Staci Eisenberg, Caroline J Kistin, Jamie Gross, Gabrielle Block, Barry Zuckerman, and Michael Silverstein. 2016. Overstimulated consumers or next-generation learners? Parent tensions about child mobile technology use. *The Annals of Family Medicine* 14, 6 (2016), 503–508.

[79] Helen J Richardson. 2009. A 'smart house' is not a home: The domestication of ICTs. *Information Systems Frontiers* 11, 5 (2009), 599. https://doi.org/10.1007/s10796-008-9137-9

[80] Frederick P Rivara, Ned Calonge, and Robert S Thompson. 1989. Population-based study of unintentional injury incidence and impact during childhood. *American Journal of Public Health* 79, 8 (1989), 990–994. https://doi.org/10.2105/AJPH.79.8.990

[81] Michael C Roberts and Penelope H Brooks. 1987. Children's injuries: Issues in prevention and public policy. *Journal of Social Issues* 43, 2 (1987), 1–12. https://doi.org/10.1111/j.1540-4560.1987.tb01291.x

[82] Johnny Saldaña. 2015. *The coding manual for qualitative researchers*. Sage, USA.

[83] Ruth Simpson. 1996. Neither clear nor present: The social construction of safety and danger. In *Sociological Forum*, Vol. 11. Springer, 549–562. https://doi.org/10.1007/BF02408392

[84] Kaiwen Sun, Carlo Sugatan, Tanisha Afnan, Hayley Simon, Susan A Gelman, Jenny Radesky, and Florian Schaub. 2021. "They See You're a Girl if You Pick a Pink Robot with a Skirt": A Qualitative Study of How Children Conceptualize Data Processing and Digital Privacy Risks. In *ACM Conference on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, 687:1–687:34. https://doi.org/10.1145/3411764.3445333

[85] Richard H Thaler and Cass R Sunstein. 2009. *Nudge: improving decisions about health, wealth, and happiness*. Yale University Press.

[86] Kentaro Toyama. 2011. Technology as amplifier in international development. In *iConference*. Association for Computing Machinery, 75–82. https://doi.org/10.1145/1940761.1940772

[87] K Tsoumakas, E Dousis, F Mavridi, A Gremou, and V Matziou. 2009. Parent's adherence to children's home-accident preventive measures. *International Nursing Review* 56, 3 (2009), 369–374. https://doi.org/10.1111/j.1466-7657.2009.00720.x

[88] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2013. The current state of access control for smart devices in homes. In *Workshop on Home Usable Privacy and Security*. USENIX Association, USA, 1–6. http://cups.cs.cmu.edu/soups/2013/HUPS/HUPS13-BlaseUR.pdf

[89] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance. In *ACM International Joint Conference on Pervasive and Ubiquitous Computing*. Association for Computing Machinery, 129–139. https://doi.org/10.1145/2632048.2632107

[90] Facebook User. 2017. You Should Consider Adding A Child Lock Feature to Future Roomba. https://www.facebook.com/irobot/posts/you-should-consider-adding-a-child-lock-feature-to-future-roombas-my-17-month-ol/10154621980033924/

[91] Reddit User. 2019. Wireless button with child safe battery compartment? https://www.reddit.com/r/homeautomation/comments/d2ok4i/wireless_button_with_child_safe_battery/

[92] Mariana Vaillant-Molina and Lorraine E Bahrick. 2012. The role of intersensory redundancy in the emergence of social referencing in 51/2-month-old infants. *Developmental psychology* 48, 1 (2012), 1.

[93] Neil Vigdor. 2019. Somebody's Watching: Hackers Breach Ring Home Security Cameras. https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html

[94] Tedra A Walden and Tamra A Ogan. 1988. The development of social referencing. *Child development* 59, 5 (1988), 1230–1240.

[95] Robomow Website. 2021. What safety features does Robomow have? https://robomow.zendesk.com/hc/en-us/articles/115005333265-What-safety-features-does-Robomow-have-

[96] Wikipedia. 2021. CE marking. https://en.wikipedia.org/wiki/CE_marking

[97] Wikipedia. 2021. HomeKit. https://en.wikipedia.org/wiki/HomeKit

[98] Wikipedia. 2021. UL(safety organization). https://en.wikipedia.org/wiki/UL_(safety_organization)

[99] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. 2015. Smart homes and their users: a systematic analysis and key challenges. *Personal and Ubiquitous Computing* 19, 2 (2015), 463–476. https://doi.org/10.1007/s00779-014-0813-0

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

[101] 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. In *ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW)*. Association for Computing Machinery, 302–316. https://doi.org/10.1145/2675133.2675293

[102] Jong-bum Woo and Youn-kyung Lim. 2015. User experience in do-it-yourself-style smart homes. In *ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*. Association for Computing Machinery, 779–790. https://doi.org/10.1145/2750858.2806063

[103] Peter Worthy, Ben Matthews, and Stephen Viller. 2016. Trust me: doubts and concerns living with the Internet of Things. In *ACM Conference on Designing Interactive Systems (DIS)*. Association for Computing Machinery, 427–434. https://doi.org/10.1145/2901790.2901890

[104] Zheng Yan. 2005. Age differences in children's understanding of the complexity of the Internet. *Journal of Applied Developmental Psychology* 26, 4 (2005), 385–396. https://doi.org/10.1016/j.appdev.2005.04.001

[105] Zheng Yan. 2009. Limited knowledge and limited resources: Children's and adolescents' understanding of the Internet. *Journal of Applied Developmental Psychology* 30, 2 (2009), 103–115. https://doi.org/10.1016/j.appdev.2008.10.012

[106] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending my castle: A co-design study of privacy mechanisms for smart homes. In *ACM Conference on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, 198:1–198:12. https://doi.org/10.1145/3290605.3300428

[107] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy perceptions and designs of bystanders in smart homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 59:1–59:24.

[108] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security and privacy concerns with smart homes. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, USA, 65–80. https://www.usenix.org/system/files/conference/soups2017/soups2017-zeng.pdf

[109] Eric Zeng and Franziska Roesner. 2019. Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study. In *USENIX Security Symposium*. USENIX Association, USA, 159–176. https://www.usenix.org/system/files/sec19-zeng.pdf

[110] Eviatar Zerubavel. 1993. *The fine line*. University of Chicago Press, USA.

[111] Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. 2019. 'I make up a silly name': Understanding Children's Perception of Privacy Risks Online. In *ACM Conference on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, 106:1–106:13. https://doi.org/10.1145/3290605.3300336

[112] Yixin Zou, Abraham H Mhaidli, Austin McCall, and Florian Schaub. 2018. "I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, USA, 197–216. https://www.usenix.org/system/files/conference/soups2018/soups2018-zou.pdf

A INTERVIEW PROTOCOL

Warm-up questions on general smart home technology ownership, placement, and use.

- What type of smart home technologies and devices do you have? What do you use them for? (Might follow up: Do you use it to connect with or control other devices?)
- What types of smart home apps have you installed on your phone? Feel free to look through the apps on your phone. What do you use them for?
- Do you have any other automation setup as a part of your smart home experiences that we haven't discussed?
  - For instance, Do you have a vacuuming robot like a Roomba, or an automated lawnmower?

Questions on parents' mental models of the safety aspect of smart home technologies.

- What are some of the important factors you consider before you purchase [smart home device]?
  - Are there any devices you thought about getting but decided not to get? Why?
  - Are there any devices you used but later deactivated? Why?
- If you friends, who have young children, also consider buying a [smart home device] and ask for your suggestions, what would you share with them regarding your experiences with [smart home device]?
- Do you talk to your children before the purchase? If yes, what do you talk about? If not, why not?
- Do you consider the potential impact that [smart home device] might have on children? If yes, what are the impacts? If not, why not?

Questions on children's smart home use and interactions.

Be aware of more than one child and ask about each child.

- How would you explain smart home technologies (e.g. Smart speakers, cleaning robots, smart appliances, etc.) to your child?
  - (If they mention smart appliances) How would you explain the differences between traditional appliances vs smart home appliances?
- I would love to get to know more about your child(ren), if you were to use three words to describe your child(ren), what would you say?
- Do your children use smart home devices? Why or why not?
  - How do your children access smart home devices?
  - Do your children have access to the smart home apps? Why or why not? How do your children access the smart home apps?
  - Do they have the same level of access as you do (or as the siblings do)? (If yes) Have you had situations where you wanted your children to have limited access, and if so, how did you handle that?
  - What does your child like to do with the smart home technologies you mentioned?
- Are you comfortable leaving your child alone with the [smart home device] when it is functioning (or in use)? Why?

- Do children know what they can or can't do when the [smart home device] is operating or when they are near the [smart home device]? (Below are optional questions depending on the type of smart home devices the participant owns:)
  - What to do or not do when the cleaning robot is in use?
  - What to do or not do when they use voice assistants?
  - What to do or not do when using the smart lock?
  - What to do or not do with the smart thermostats?
  - What to do or not do with the security system or camera?
  - What to do or not do when plugging something in or unplugging something?
  - What to do or not do when they hear a surveillance camera notification sound?
  - What to do or not do when they hear the smart doorbell ring?
- (If safety is not mentioned yet) One factor we're interested in about smart home devices is its safety with children. Some parents have safety issues or concerns regarding smart home devices and children's interaction with them.
  - Do you or did you have any concern about children's safety when it comes to smart home devices?
  - Are your children aware of such safety risks? How do they feel about these safety risks?
  - (Optional) Have you heard any smart home safety concerns with children from friends, in the news or other sources? If so, how do you feel about such news? Did that news concern you, or do you think those issues are a little overblown?
- (If previous answers haven't touched on safety characteristics of smart home devices) What would you consider safe or unsafe about a smart home device?
  - Do you consider [smart home device] safe or unsafe for your child? In what ways? Why or why not?

Questions on the challenges between children and smart home technologies and parents' corresponding mitigation strategies.

- Have your children voiced any opinions or concerns about the smart home technologies? How do you respond to their opinions or concerns?
  - Are there any challenges you see when your child interacts or uses [smart home device]? What have you done in response to that challenge?
  - Is there anything you worried about the way your child uses or interacts with the [smart home device]? Why?
- Have you ever had disagreements with your children about how your smart home devices are set up or used? If yes, what are they? How did you resolve the disagreement?
- Do you have any rules for your children regarding whether they can or can't use these smart home devices or not?
  - If yes, do the rules apply to all smart home devices or are specific for certain types of devices or uses?
  - Why are these rules important?
  - How did you come up with these rules?
  - How do your children react to these rules?
  - Are there times that your children disagree with or don't follow the rules? If yes, what would you do?

Closing questions.

- What kind of features, functions or controls that the [smart home device] should have to alleviate your concerns regarding children's safety? Or, what kind of features, functions or

controls would you like to have in your smart home to alleviate your concerns regarding children's safety?
- Are there any questions you expected me to ask?
- Is there anything else you want to tell me about your children and your smart home devices?

B SCREENING SURVEY

(1) What type of smart home technologies do you have in your household?
  - Video Entertainment: smart TV, Apple TV, Chromecast, etc.
  - Home monitoring/security: security cameras, smart lock, video doorbell, baby monitor, etc.
  - Smart speaker
  - Smart light
  - Smart blind
  - Smart switch/outlet/button
  - Smart thermostat
  - Smart cleaning robot
  - Kitchen appliances of all sorts: smart pot, smart coffee maker, smart fridge, smart microwave, etc.
  - Smart washing machine
  - Smart pet/plant care
  - Smart mower
  - Remote controllable doors (including garage door)
  - Smart home gym equipments
  - Connected car
  - Other (please specify)

(2) Please select the type of devices that your child(ren) have been in contact with, interacted or used before. [Provide the same list as in Q1]

(3) For your child(ren) who have been in contact with, interacting with, or using the smart home technologies, how old are they? [Open-ended]

(4) Please leave your contact information (name and email address) so we could reach out to you. [Open-ended]

(5) If you are willing to be contacted for participation in future research projects that may be relevant to this research project, please click the consent option below. (If you don't check this box, we consider you don't want to be contacted for participation in future research.) [Checkbox with text: I consent to be contacted for participation in future research.]

C CODEBOOK

Table 2. Codebook on children's perceived mental models and attitudes.

Code	Description	Example Quotes
Observed readiness to own or control smart home tech	Parents thought their children are trustworthy or capable of using smart home devices or not. Can include cases of non-use if it's implied that children are following what they're supposed to do.	*"They're five and seven. I highly doubt anything suspicious is going down. I'm more reactive at this point. [Checking audio logs on the smart speaker] is something that I would do proactively when they were older and capable of making graver mistakes or if I had some kind of instinct that they were not being honest with me right now."*
Children's risk awareness regarding smart homes	Parents mentioned their children's awareness of any types of risks such as those related to safety, privacy, and security. Also include general online risks outside of smart home devices such as those in using social media or mobile apps.	*"I guess he probably has like a real fledgling awareness of 'there are other people online and they're not always friends.' But no, I don't think they have any real concern about [safety]."*
Children's challenges with smart home devices	Parents mentioned how their children have opinions, concerns, or challenges with smart home devices.	*"They're not in any way patient. So if they press a button on the switch, they expect results in 100 milliseconds. If things don't respond very quickly, they will repeatedly press the button until such time as they either get the desired response or something else unexpected happens."*
Children's perception of smart home tech	Include children's perception of what smart home tech is (e.g., perceive a smart speaker as a robot) and attitudes (e.g., love the smart speaker). Include cases of misconceptions (e.g., think a smart home device is capable of doing X but in reality it doesn't).	*"They know that Alexa is a computer. I don't think they have a solid grasp on what a computer is ... or why a light switch can be a computer."*

Table 3. Codebook on children's perceived behaviors.

Code	Description	Example Quotes
Children's interactions with smart home devices: stream media	Examples include playing Lord of the Rings soundtracks, streaming Netflix, Etc.	*"They haven't been using [smart home tech] very much. It's mostly the Echo Dot ... streaming TV services of Netflix and Amazon Prime on the little Smart TV input."*
Children's interactions with smart home devices: ask questions	Examples include asking the smart speaker to spell a word or tell a joke.	*"When they're doing homework. Sometimes if they don't know a word, they actually ask Google to spell the word ... Sometimes they try to cheat on math homework as well, but I usually discourage that."*
Children's interactions with smart home devices: control the lights	Examples include using voice commands to interact with smart switches or buttons, or controlling the lights using smart home hubs.	*"We have smart lights installed in their bedrooms, so that first thing in the morning they can turn on their lights by asking ... or if they get up in the middle of the night and are scared of the dark ... they can ask it to be turned on."*
Children's interactions with smart home devices: check the camera	Examples include using the camera to see who's at the door or check how siblings behave through the baby monitor.	*"We have a video doorbell, so anytime it rings ... the kids can check our phones and the Nest Hub to see who is at the door."*
Children's interactions with smart home devices: control door locks	Parents mentioned their children interacted with a smart lock physically (e.g., by entering a password on a keypad) or remotely (e.g., through a smart home app).	*"They would be home for about an hour or two before my husband or I got home from work ... They were using a keypad to get in through our garage."*
Children's interactions with smart home devices: other	Examples include using smart home devices to set timers, having video calls with other people, and any other instances that do not fall under the codes above.	*"We also have a Facebook Portal which we've used to talk to people, and then he's very familiar with using FaceTime."*

Continued on next page

Code	Description	Example Quotes
How children access smart home devices: phone or tablet	Children can access (or not) smart home devices through their phone / tablet or those owned by their parents.	*"They do have tablets. They each have a Chromebook ...and an iPad. But none of those are integrated into smart homes and none of them have apps to control anything in the house."*
How children access smart home devices: smart home hub	Children can access (or not) smart home devices through a smart home hub (e.g., Amazon Echo Dot or Samsung SmartThings Hub) in their home.	*"We have two Google Minis and a Google Home Hub, which is the one with the screen. So all the kids use the voice commands for things or even ... set up a timer for a timeout."*
How children access smart home devices: voice commands	Children use voice commands (or not) to access smart home devices, mostly smart speakers. Can be double coded with the interface of access.	*"They like to hear the stories, and I don't know how we stumbled upon it, but they'll say like 'Alexa, tell me a story' when we're just sitting around."*
How children access smart home devices: physical controllers	Children use physical controllers (or not) to access smart home devices such as smart switches, buttons or TVs. Can be double coded with the interface of access.	*"If they really need to turn the light off and on ... they would use their voice or actually go to the switch and turn [it] off. They wouldn't touch [the Google Nest Hub.]"*
How children access smart home devices: other	Other interfaces or mechanisms children use (or not) to access smart home devices.	*"Both of our phones have passcodes on them, or fingerprint or face ID ... She is not authorized using the biometric stuff and as far as I know, does not know the passcodes."*
Sibling influences: copy each other	Children copy or learn from their siblings' behaviors in interacting with smart home devices.	*"The younger one is just copying the older one ... learning how to make it listen. So she's trying the 'OK Google' over and over again to try and get it to respond, because she sees her sister doing that."*
Sibling influences: conflicting use	Children compete for ownership, fight for turns, or show conflicting preferences in using smart home devices.	*"Sometimes our older son gets annoyed with the other son if he keeps asking it to play the same song ... There's conflict about what music to listen to. Our third child likes to listen to the same thing over and over again. It gets on the older two's nerves."*
Sibling influences: other	Other instances that show interactions or influences between siblings in smart home usage, such as using smart home devices for pranking or monitoring.	*"It'll happen sometimes when the younger one will notice the older one playing [through the camera] and say, 'What's he doing? ... Is he playing with my stuff?' They will check on each other."*
Children's reaction to parental rules	Children follow or disobey rules given by parents about how they should use smart home devices. The focus is on children's reactions, not the rule's content.	*"I think they understand it, and they trust us. They follow the rules a lot, to the point where they won't even watch movies with us that are maybe borderline."*

Table 4. Codebook on parents' mental models and attitudes.

Code	Description	Example Quotes
Smart home purchase considerations: price	Parents considered price in making the purchase, e.g., going after cheap, cost-effective products or avoiding expensive products.	*"If you ever priced out blinds, it's absurd ... It may be like $200 for a ruler shade ... $800 for one window, and you're dropping $1,000 just to put a smart roller blind sheet on one window. That's why I haven't rushed out to do that."*
Smart home purchase considerations: brand	Parents indicated they trust certain companies or brands when making the purchase, or indicated if they get a new product in the future, it's because they trust the manufacturer.	*"My light switches are all Lutron, and I kind of defaulted into that ... I discovered that the Lutron company has been doing home automation for close to 30 years ... As I expanded my system without awareness, I tried to use their products as much as possible."*
Smart home purchase considerations: privacy	Parents considered the product's privacy implications, e.g., buying the product with strong privacy protections for consumers or avoiding the product due to privacy concerns.	*"Number one is privacy. Despite the fact that I literally worked for one of the cloud companies, I do not want them to have any of my data about how we move around our home."*

Continued on next page

Code	Description	Example Quotes
Smart home purchase considerations: security	Parents considered the product's security features or benefits, e.g., buying the product since it makes the home more secure or avoid the product due to security concerns.	*"One of the biggest drivers for us doing any smart home stuff is around . . . security in the home. In fact, our smart home process started because I am so horrifically bad at remembering to lock doors."*
Smart home purchase considerations: safety	Parents considered the product's safety features or benefits, e.g., buying the product because it enhances home safety or is safe to use. Can be double coded with security.	*"With the Apple Home Kit system framework, there are actually some security requirements baked into that . . . So at least the Home Kit stuff gives me a sense of safety, that there is some security baselining supply to it by default."*
Smart home purchase considerations: compatibility	Parents considered the product's compatibility with their existing smart home system in making the purchase.	*"Integration into one or more of my existing platforms is pretty crucial; multiple platforms is a bonus."*
Smart home purchase considerations: reliability	Parents described considering whether the product is reliable and can work consistently over time when making the purchase.	*"My highest priority is reliability. It has to work basically 99.99% of the time. If an automation or switch or something like that doesn't work one time out of 10, everybody in my house will hate it."*
Smart home purchase considerations: functionality	Parents described considering the product's functions, features, or the potential convenience it could bring to the home when making the purchase. Examples of device features include whether the device needs a particular network or whether it relies on a hub to work.	*"Now, I am more focused on functionality. Like, does this solve a problem in the household? Does this make things easier for the kids or for myself, for my wife? What's the cost associated with that?"*
Smart home purchase considerations: ease of use	Parents considered whether the product is easy to use for general users (not specific to children) in making the purchase.	*"Number two is what people often refer to as the wife acceptance factor . . . A less misogynistic version of that term would be like user experience . . . User experience is absolutely critical."*
Smart home purchase considerations: children's use	Parents described considering whether the product is useful for children, whether it's easy to use for children, whether children will be addicted to or abuse it, etc. when making the purchase.	*"As a parent . . . the parental controls or access controls would be something I would think about . . . Is it something that I can use, but the kids can't? Or is it something that I can limit their access?"*
Smart home purchase considerations: other	Parents described considering other factors that are not captured by the codes above in making the purchase, such as the time required to set up and configure the device or their tendency to make impulse purchases.	*"The thing I really like about smart home stuff is that smart homes move a lot slower than other tech products like phones, and it feels a lot easier to invest in it . . . It shouldn't have to be something that you're reinvesting in every three years."*
General concerns: privacy, security, or safety	Parents described general, not children-specific concerns about smart homes regarding privacy, security, or safety aspects, such as no indoor cameras to protect the privacy of nannies or worries about the device being hacked.	*"We have more than one in-home employee. The kids have a nanny, and there's also a medical aid that assists with one of my children . . . Out of respect for them, we don't have our cameras inside the home."*
General concerns: device functionality	Parents described general, not children-specific concerns that a smart home device does not work as expected and malfunction situations could occur.	*"The biggest problem with the doorbell is that it's [connected to] WiFi and it's battery operated. And the WiFi beats the battery up pretty quickly. So we get like a couple days worth of doorbell operation and then it's done."*
Trust in smart home companies	Parents described they trust a certain smart home company or feel comfortable with using the company's products.	*"I can easily opt out of Siri sending those things that it records. Apple has gone all the way to the Supreme Court to defend an individual's rights in their own information, which makes me feel [it is] at least somewhat more willing to be private than the other companies."*
Distrust in smart home companies: trust	Parents described they distrust a certain smart home company or feel uncomfortable with using the company's products.	*"Facebook and Google and Amazon are all like, 'Oh yeah, we're taking great care of your kids!' No, you're not. [It's] very clear that you're doing your best, but the technology is not there yet."*
Perceived impacts on children: privacy	Parents described how the privacy implications of smart home devices could impact their children, e.g., by causing information leaks or chances of their children being spied on.	*"I just don't want someone seeing the kids . . . You do hear horror stories of like talking to them over the monitors and things. So I guess that's a concern of mine."*

Continued on next page

Code	Description	Example Quotes
Perceived impacts on children: security and safety	Parents described how their children's security and safety could be impacted when they use smart home devices, e.g., exposure to explicit, scary, or child-inappropriate content.	*"It's nice to be able to monitor the kids when we're working or when we're not around them ...But then I thought if there's something like a security breach, then I'm sure someone else can access that feed."*
Perceived impacts on children: exposure to ads or profiting content	Parents described concerns about their children being exposed to ads or profiting content when using smart home devices.	*"YouTube kids is one thing that I've banned in the house ...It turns them into little addicts ...He was so fixated [that] the one or two times he used it, it was just such a fight to get it away from him ...All those toy videos ... What are these people really producing this content? It's just for money."*
Perceived impacts on children: other	Other potential impacts of smart home devices on children as parents perceived, including both positive and negative cases.	*"I wonder, for the future, if they're going to demand that everything is smart in houses for apartments that they rent ...That's why we're trying to keep as much interaction [of] manual use as possible so they don't grow up thinking that they have to have their smartphone to turn on the light."*
Leaving children with smart home alone: comfortable	Parents said they would be comfortable with leaving children alone with smart home tech.	*"I'm confident in their ability to generally operate them correctly. I don't have a lot of safety concerns ...mostly because I trust the kids ...At this age, they're not going looking for anything inappropriate. They're not trying to sneak anything past me that's dangerous."*
Leaving children with smart home alone: uncomfortable	Parents said they would have concerns or reservations when leaving children alone with smart home tech.	*"Not yet ...He's nine ...and like I said he's proven to be pretty responsible. I think that time is coming really soon ...I just want to make sure that he's ready for it."*
Existing features that enhance user experience	Parents' mentioning of any particular resources or features about smart home tech that would provide a positive user experience or help parents better manage their children's access.	*"The ability to ... set hours when it just does not respond is handy. So between eleven and seven ... that speaker will not listen to anyone except the adults. So that they can't get up at two in the morning and decide they really want to watch Paw Patrol."*
Existing features that increase safety	Specific features mentioned by parents that make smart home tech safe for children to interact with.	*"To close the garage door, there's a safety feature where for like 10 seconds the light in the garage starts blinking and beeping, so that if someone is under the garage door they would know someone accidentally or intentionally is closing the garage door."*
Existing features that decrease safety	Specific features mentioned by parents that make smart home tech unsafe for children to interact with.	*"Real danger starts to emerge with mechanical action ...Say we're gonna have the door be motorized and remote controllable, and you could have someone get their arm caught in it."*
Desired features	Specific features mentioned by parents that would better help or protect their children as smart home users, improve the overall user experience, or help parents better manage what children can access.	*"I thought the switches around our house [would need] some form of programmable vocal feedback. Like an LED that I can change the color of."*

Table 5. Codebook on parents' behaviors.

Code	Description	Example Quotes
How parents access smart home devices: phone or tablet	Parents described accessing (or not) smart home devices through the apps on their phones or tablets.	*"I have a smartphone. The doorbell, if we want to, we can open up the Ring app to see through the camera."*

Continued on next page

Code	Description	Example Quotes
How parents access smart home devices: smart home hub	Parents described accessing (or not) smart home devices through a smart home hub (e.g., Amazon Echo Dot or Samsung SmartThings Hub) in their home.	*" I piecemeal things together with Alexa, because I'm assuming Amazon charges basically nothing, and it charges more to integrate into your apple home system . . . I just kind of fidget around with multiple apps that are kind of integrated to Alexa."*
How parents access smart home devices: voice commands	Parents described using voice commands to access smart home devices. Can be double coded with the interface of access.	*"Sometimes I'll ask Siri to do something, where I say, 'play my list' or 'turn on my lights.' It'll say, 'I don't know who you're talking about.' Then I identify myself and then the automation will go and run."*
How parents access smart home devices: physical controllers	Parents described using physical controllers (or not) to access smart home devices. Can be double coded with the interface of access.	*"They don't know how to do that . . . I just take care of entering the pin number on it and open it."*
Childproof smart home devices: yes	Parents described childproofing smart home devices when their children were young.	*"We didn't put the devices in the kids' rooms until after they were walking, just so that they wouldn't use the cord to . . . pull themselves up or anything like that . . . Now all of the cords are wrapped up, so there's no [chance] that they can . . . hurt themselves."*
Childproof smart home devices: no	Parents said they did not childproof smart home devices when their children were young or they could not remember doing it.	*"No, our kids always listened. So we only childproofed as needed. We put the knives up higher. We had one baby gate . . . [But] we never had to childproof the smart devices. We were never really worried about it."*

Table 6. Codebook on parent-child interactions.

Code	Description	Example Quotes
Children's involvement in purchase decisions: before purchase	Parents mentioned that they had talked to children before buying a smart home device that's intended for children or would involve children when being used.	*"If it particularly involves them, I want to double check with them to make sure that the use case actually exists . . . like, 'Hey, would you like this thing in your room?'"*
Children's involvement in purchase decisions: after purchase	Parents mentioned that they would introduce the device to children and explain rules of use after making the purchase.	*"We purchased it and set it up, then we talked about it. We make the decisions first. He's really young . . . and he's going to want all the latest and greatest."*
Children's involvement in purchase decisions: no involvement	Parents mentioned they did not involve children at all before or after the purchase decision.	*"The last time I bought [a smart home device] . . . they were probably too young to have that conversation. I think if I did now, I probably would explain anyway."*
Conflicts over smart home use	Parents mentioned conflicts or disagreements they had with children in setting up and using smart home devices (excluding conflicts among children themselves).	*"They sometimes can get fixated on it . . . A very common thing at dinners is like 'All right, we're done.' And I just pull the plug on the [Amazon Echo] Show, and they'll say 'Oh you don't have to unplug, I'll stop now. I really will.'"*
Children copying parents' behaviors	Parents mentioned their children would observe how they interacted with smart home devices and mimic such behaviors.	*"Our son has just turned two, and he'll basically try to simulate or copy us . . . I always speak loudly and clearly, so I kind of raise my voice and try to enunciate. Then he will copy me and will try to shout the word 'Alexa.'"*
Education / guidance about rules: screen time	Parents described efforts in communicating with or educating their children about proper screen time and not getting addicted to technologies.	*"We're cognizant that if it was up to them, they would be on those things all the time. So we have a cap of 30 minutes a day, then they have to earn enough credits to be able to have that screen time each day."*

Continued on next page

Code	Description	Example Quotes
Education / guidance about rules: privacy, security, or safety	Parents described efforts in telling children what to watch out for regarding privacy, security, and safety in using smart home devices.	*"We've also had conversations about not sharing that information and 'don't talk to strangers,' but on a really basic level."*
Education / guidance about rules: proper use	Parents described efforts to help children feel more comfortable using smart home devices, form good habits or behaviors, or "do the right thing."	*"The thing where my son thinks is funny [is] to turn off all the lights when someone else is going into that part of the house. I told him, 'okay, that was funny once, but we're not going to keep doing that.'"*
Education / guidance about rules: other	Other educational efforts from parents that are not captured by the codes above.	*"We don't have any rules in place right now. We've opted instead for sort of behind-the-scenes control . . . I expect somewhere down the road, we will have to introduce the concept of sharing especially when it comes to what they want to watch."*
Mitigation strategies: non-disclosure	Parents intentionally avoid telling their children the existence of certain smart home devices or features (including hiding certain apps from the interface).	*"If he knew about [the thermostats], and if he knew that he could control them, then he could because there's no way to prevent him from doing it. And so I just haven't told him about that stuff."*
Mitigation strategies: forbid access	Parents didn't give children access or forbade them to use certain devices such as thermostats and security alarms. The children would lose access rather than have limited access (e.g., when parental control features are implemented).	*"If we had smart sprinklers, I obviously wouldn't give them access to things like that. It's . . . what they can do with that device that I'm more concerned about."*
Mitigation strategies: DIY automations	Parents discussed how they modified smart home features to cater to children's needs or make it difficult for children to abuse the system.	*"I got motion sensors that trigger things depending on the time of day . . . For example, I have a sensor that if you walk into the bathroom between midnight and 5:30 . . . it'll turn the lights on for you."*
Mitigation strategies: use parental control features	Parents mentioned using built-in parental control features on device or repurposing a feature for parental control purposes, such as automatically filtering explicit content and restricting screen time to only certain hours.	*"We have family [accounts] set up through Google that restrict some access on the smart speakers, and we filter out explicit videos."*
Mitigation strategies: other	Other mitigation strategies not mentioned in the codes above, such as making the device hard to reach and unplugging the device.	*"If she kept on wanting to listen to something, I would say 'no we're not doing that right now.' Then I would hit the mute button on it so that even if she kept asking, it wouldn't respond."*
Changes as children grow up	Parents discussed hypothetical scenarios in which their children have grown up and they would need to adapt their parenting accordingly, e.g., by limiting or allowing the children's access to different devices.	*"To me, I can't control what they're going to download when they're 13, I'm going to have to let go. The only thing I can do . . . for the next five years until they turn 13 is [to] instill in them this sort of natural skepticism."*

Received April 2021 ; accepted July 2021