Laughing is Scary, but Farting is Cute

A Conceptual Model of Children's Perspectives of Creepy Technologies

Jason C. Yip, Kiley Sobel, Xin Gao, Allison Marie Hishikawa, Alexis Lim, Laura Meng, Romaine Flor Ofiana, Justin Park, Alexis Hiniker

University of Washington

Seattle, WA United States

{jcyip,ksobel,xin24,allikawa,alexisl,lxmeng,rfo,justin38,alexisr}@uw.edu

ABSTRACT

In HCI, adult concerns about technologies for children have been studied extensively. However, less is known about what children themselves find concerning in everyday technologies. We examine children's technology-related fears by probing their use of the colloquial term "creepy." To understand children's perceptions of "creepy technologies," we conducted four participatory design sessions with children (ages 7 - 11) to design and evaluate creepy technologies, followed by interviews with the same children.

We found that children's fear reactions emphasized physical harm and threats to their relationships (particularly with attachment figures). The creepy signals from technology the children described include: deception, lack of control, mimicry, ominous physical appearance, and unpredictability. Children acknowledged trusted adults will mediate the relationship between creepy technology signals and fear responses. Our work contributes a close examination of what children mean when they say a technology is "creepy." By treating these concerns as principal design considerations, developers can build systems that are more transparent about the risks they produce and more sensitive to the fears they may unintentionally raise.

CCS CONCEPTS

• **Human-Centered Computing → Collaborative and Social Computing**; • **Human Centered Computing → Human Computer Interaction (HCI)**.

KEYWORDS

Children and Parents, Creepy, Fear, Threats, Privacy and Surveillance, Participatory Design

1 INTRODUCTION

Children frequently encounter new information communication technologies that are novel and innovative, but also unknown, unfamiliar, and potentially scary. In HCI, although adults' concerns about technologies for children have been studied extensively - including fears about children's privacy, security, and online safety (e.g., [16, 18, 55–57, 94, 100]) - less is known about what children themselves find concerning or disturbing in the technologies they encounter in everyday life.

Although it is essential to understand parents' fears and to define policies that are sensitive to the whole families' needs, there is also a need to further examine children's perspectives of a fast-changing world of technology and how it relates to fears and apprehension in childhood [43]. By understanding children's perspectives of the relationship between fear and technology, we can make better evaluations and designs for children. Understanding children's perceptions and expectations of technologies matters as much as parental perspectives since families use technologies together [15, 86, 87]. To understand children's perspectives of creepy technologies, it is necessary to develop a conceptual model of how children think about the technologies that surround them.

We examine children's perceptions of fear through the colloquial term of "creepy." We chose to examine children's perceptions of creepiness because it is an all-encompassing everyday word that covers topics of threat, fear, strangeness, weirdness, unpredictability, and the unknown [63, 88]. In our

research on child-computer interaction, children in our studies and design sessions often used the word "creepy" as a way to convey negative feelings about design and technology. Surprisingly, creepy as a term has just recently been defined and studied [63, 88]. We aimed to answer two research questions:

RQ1. What do children consider disturbing or unsettling about the technologies they encounter? What properties signal to a child that a technology does not deserve their trust?

RQ2. When children find a technology creepy, what is it that they are worried about?

To understand how children conceptualize how technologies can be creepy, threatening, and fearful, we conducted four participatory design (PD) sessions and a set of interviews with an intergenerational co-design group of 11 children (ages 7-11, with at least eight of these children present at each session). The sessions concentrated on co-designing creepy and trustworthy technologies and evaluating a series of technological scenarios. We used a different design activity for each session to elicit how children conceptualize fear and technologies.

We contribute to the discussion on children, fear, and technology in three ways. First, we report a set of design categories that signal to children that a technology is creepy. Second, through the development of a conceptual model of creepiness, we show links between these design signals and the fears they instill. Finally, we provide parental recommendations for managing technologies in the home and design recommendations to prevent the inadvertent design of creepy technologies.

2 BACKGROUND

Childhood and Normal Fear

Fear is needed as an integral and adaptive aspect of development that warns organisms to flee danger [43]. From an evolutionary perspective, fear is needed for humans to survive dangers, such as predators [35], contamination and contagion [34], status threat [78], and violence [50]. Extensive research into "normal fear" in childhood spans over a century [42]. Normal fear, defined as an adaptive response to real or imagined threat, is one of the most researched emotions in children [42, 43]. In developmental psychology, there are typical fears that show up in stages in childhood. In early childhood (18 months to 5 years), children are able to explore the world more. This means that fear transitions even more towards stranger anxiety [21, 30] and adaptations to the world [19]. Towards middle childhood (ages 6-9 years), fear develops against monsters and mysterious intruders [82] with much of these fears influenced from cultural aspects

like myths, stories, fairy tales, and mass media [49]. In middle to late childhood (ages 9-12 years), social anxieties and worries take place, such as loss of friendship, betrayal, and the beginning of social threats online [26, 32, 92].

Despite diverse cultures, environments, and social status, threats and fear development in children are quite stable across humans [19]. This can be seen in early and middle childhood fears of bedtime and isolation across cultures [48, 77]. Interestingly, children are more fearful of potential and probable threats, than actual threats [19]. However, children are not irrational or misguided. Boyer and Bergstrom's [19] review found that children's fears correspond and come to fruition when actual dangers begin to occur in their lives. Children and adults are also similar in respect to fear of dangers that are not part of their direct world. Fear is not just an inherently biological response to the world, but also part of the learning system of a child [12–14, 17]. Children can vicariously learn to fear, even without direct contact with fear stimulus [12–14]. As such, it is important to consider how technologies over time can develop as part of children's fear.

Families, Technologies, and Fear

More recently, with the growing use of technology in the home, both parents and children have developed an increased awareness of safety, as well as anxiety [18, 51, 84]. Marwick [61] calls this new fear, "technopanic," that is "an attempt to contextualize the moral panic as a response to fear of modernity as represented by new technologies." The rise of modernity and unknown technologies has increased parents' own fears [84]. As parents become increasingly fearful, this can trickle down to the development of children's own fears [14, 71]. The research on fear of technology in HCI has focused mostly on parental fears of technology for their children and how to protect children. Parents have many fears about online privacy, surveillance, safety, visibility [16, 18, 36, 89, 94], screen time addictions [38, 39, 58], and explicit media content [16, 36, 94]. Unsurprisingly, parents employ a number of strategies to keep their children safe from threats, such as parental monitoring and surveillance [18, 36, 37, 94] and mediation strategies [24, 58, 59, 66, 90]. More recently, HCI researchers have co-designed with children safety strategies and self-regulation [56, 64]. Despite some tensions with parents and children when it comes to how to execute online regulation [16, 18], children do acknowledge that parents should be regulating their online safety and rules [56, 64].

While much literature exists on how parents perceive fear and safety, less is known directly about children's own fears of technology. More recently, Zhang-Kennedy et al. [100] focused on parent-child dyads to explore children's (ages 7-11) perceived privacy and security threats. The researchers noted

that technology fears and threats from children quite differed from parents. For instance, children thought friends, siblings, and classmates were threats because the other children could get them into trouble with adults. Children thought that it was dangerous to be exposed to violent and explicit media content because they might get in trouble with other adults, such as teachers and parents. Newer internet-connected technologies and toys are also a possible new source of fear in children. McReynolds et al. [65] found that children were not always comfortable playing with internet-connected toys (Hello Barbie, Cognitoys Dino). Children (ages 6-10) had privacy expectations of the toys, and did not always feel comfortable sharing "secrets" with a toy that could listen in. There is a need for children to learn more holistically about what fears children have, even if the fears are potential. It is also important to understand how to help children mediate their own fears and safety online and develop strategies to help parents mitigate both trust and control [45], as well as what role interaction designers play.

The Nature of Creepiness and Technology

To better understand children's fears of technologies, we chose to use the colloquial word "creepy" as a way for children to both examine and express their fears. Prior work defines creepiness as the anxiety aroused specifically by ambiguity surrounding a potential, but uncertain, threat [63]. In contrast, scariness is more closely linked to direct and certain threat [43]. For instance, a "creepy" sensation of being watched relates to the uncertainty of how that person should respond. This ambiguity stands in stark contrast to the sensation produced by being chased by a "scary" monster, an act that demonstrates clear threat. Both creepy and scary stimuli can provoke fear responses in children [43], but the presence or absence of ambiguity makes these two forms of fear response qualitatively different [63].

In 2016, the first scientific paper to examine the nature of creepy focused on a survey of 1,341 adult individuals [63]. For adults, creepy is a gendered term; people perceive men to be creepier than women, particularly as a sexual threat from a creepy person. Unpredictability is an important component for creepy, such as laughing at unforeseeable and odd times. Finally, some hobbies and interactions are strongly associated with creepy, such as watching and following people, photographing people (especially children), and fascination with pornography and taxidermy.

A link exists between creepiness and technologies. Tene and Polonetsky [88] developed a theory of creepy in technology interactions. In their theory [88], creepy, as it pertains to technology, policy, and law, is not unlawful. In fact, creepy technologies are not always harmful, do not directly circumvent privacy settings, and do not always excessively collect data. Their theory states that creepy technologies

tend to push against traditional social norms, expose a rift between the public and the designers/engineers/marketing professionals, and do not (yet) have social norms around the technology.

In HCI, creepiness has been studied in the space of how users felt privacy violations and personal space in the Apple App Store [83], privacy concerns in online advertisements [67, 75] and user perceptions and trust in online privacy disclosures [60]. Two studies exist on children and creepiness in technologies. Brink et al. [20] examined the uncanny valley in youth (ages 3-18) in human-robot interactions. The uncanny valley is a phenomenon in which as robots become more human-like, people see them as strange and weird [68, 69]. Brink et al. found that children had uncanny feelings about human-like robots, especially if they have human-like minds [20]. Another study described children's mental models of how Google's search engine works, related to a picture of a "creepy guy" at the other end of a computer that sent the children the search results [53]. Overall, much less is known about children's perceptions of creepy technologies, how it relates to fears and threats, and how children mediate this tension.

3 METHOD

Participatory Design

For this study, we adhered to the participatory design (PD) method of Cooperative Inquiry [28, 98]. PD is a method of design that brings users and designers together to co-design new technologies [31, 52]. Cooperative Inquiry is a method of PD that emphasizes close design partnerships between children and adults [28, 98].

We chose to use PD and Cooperative Inquiry [28, 98] as our method for this investigation for three reasons. First, prior research has shown that while interviews and surveys are scalable for fear studies (i.e., more children can be inquired) [42], the complex and sensitive nature of fear, creepiness, and technology can be difficult to elicit responses through interviews alone [93]. Second, researchers in HCI have demonstrated that PD techniques allow children to more concretely express abstract ideas [29, 40, 41, 91, 95]. When considering complex technological interactions for children, such as their perceptions of fear and creepiness, interviews and surveys alone do not generate as rich of data as PD techniques [91, 95]. We believe that to initially develop a conceptual model of fear and creepiness, we needed methods of design with children that allow for in-depth rich engagement.

Cooperative Inquiry works well for fear and creepiness for three reasons. First, the children already work closely with adults and are more likely to express their perceptions

around childhood fear more assertively. In design partnerships, there is a strong emphasis on relationship building between children and adults [98], which allows children to be more open to adults about sensitive topics like fear, threats, and creepiness. Second, children in long term co-design groups are already knowledgeable on multiple PD techniques that can elicit different responses. Finally, Cooperative Inquiry partnerships with children have already shown to produce in-depth and rich data around complex topics of intelligent user interfaces, cyber-security, and online safety and privacy in HCI research [56, 64, 95].

Our PD sessions focused on designing and eliciting responses from children about their perceptions of creepy technologies. We conducted four 90-minute sessions across the span of six months. We used three PD techniques [91]: *Bags of Stuff* [27], *Big Props* [91], and *Line Judging* [91]. In addition, we interviewed eight out of eleven children individually to triangulate our findings between individual and group perspectives [25].

Participants

An intergenerational co-design group, consisting of both adult design researchers (investigators, masters, and undergraduates) and child participants (*n* = 11; ages 7-11) participated in the four design sessions. The team is called *KidsTeam UW* (all child names are pseudonyms, Table 1). At the time the work was conducted, all children had participated in KidsTeam UW for the past 1-4 years. We obtained parental consent and child assent. All research conducted with children has been approved by our university's Institutional Review Board for ethics. In each of the design sessions, between six and eight adult facilitators acted as design partners (e.g., designing with the children, facilitating discussions).

Design Sessions and Interviews

Each design session of KidsTeam UW consisted of *snack time* (15 minutes) to build relationships with the children. Next, *circle time* (15 minutes) is a warm up activity in which we ask a "Question of the Day" to help adults and children get ready for the design activity. During *design time* (45 minutes), the team either breaks up into smaller intergenerational groups or remains together in a single design activity. Finally, in *discussion time* (15 minutes), different groups present their final designs and the whole team reflects on the design experience and common threads. For each design session, we chose a design technique that corresponded to the goals of the session.

We organized the sessions to start broadly about what children thought about the relationship with creepiness and technology (DS1), and later focused on creepy scenarios (DS2) and real-life technology prototypes (DS3). Finally, we triangulated the sessions by asking children to develop trusting

Table 1: Demographic characteristics of our child participants. All names are pseudonyms. Siblings are indicated with +, $, # symbols.

Name	Age	Gender	Ethnicity	Sessions
Sushi	9	Female	Asian-Black	1-4, I
Raymond	7	Male	Asian	1-4, I
Justice+	10	Male	Native American-Asian	1-3
Lily+	7	Female	Native American-Asian	2,4,I
Polly$	10	Female	Asian-White	1-3
Maggie$	7	Female	Asian-White	4, I
Akane#	11	Female	Asian-White	1-3
Kenshin#	7	Male	Asian-White	2, 4, I
Alejandro	8	Male	Hispanic	1-4, I
Daniel	10	Male	White	1-4, I
Grace	7	Female	Asian	1-4, I

technologies (DS4) and interviewed them. For each design session, we video and audio recorded the interactions with a single camera. In DS1 and DS4, a rotating facilitator moved the camera throughout the session to focus on different co-design groups, while in DS2 and DS3, the camera stayed in fixed position to capture the entire group. Each design session consisted of a design activity chosen for its potential to explore different aspects of fear, creepiness, and trust.

Design Session 1 (DS1, February 2018): We asked the children to design a technology that would be creepy, but that people would want to buy. In introducing the topic of creepiness, we asked the children to design what they thought was creepy. We did not provide them with a definition, and we explicitly told them we wanted to learn what creepy means to them. We used the PD technique *Bags of Stuff* [27], a low-fidelity prototyping technique. We filled large bags with craft materials (i.e., construction paper, markers, stickers). Smaller groups of three to four children and adults worked together to create a low-tech prototype.

Design Session 2 (DS2, March 2018): We elicited information regarding how children thought about specific technological scenarios. Prior to DS2, the first and last author examined the prototypes from DS1 and developed 12 hypothetical scenarios of technologies for the children. We developed these hypothetical scenarios by pairing initial creepy themes (visual appearance, deception, privacy and surveillance, lack of control, inappropriate contexts, and mimicry) we found in DS1. For example, one scenario was a stuffed animal cat (i.e., Pusheen, Figure 1b) (physical appearance as cute) that would remind children to exercise all the time, but the children could not turn this feature off and the device sent reminders to parents about exercise status (lack of control). Another scenario was using K-2SO, a black-colored robot from *Star Wars* [47]. (Figure 1a, visual appearance as
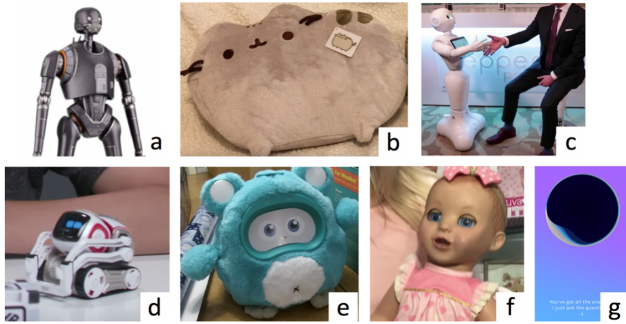
Figure 1: (a) K-2SO toy; (b) Pusheen toy; (c) Pepper robot; (d) Anki Cozmo robot; (e) Woobo; (f) Luvabella doll; and (g) Maslo app. Images captured from YouTube and Apple App Store.

fearful), and having it laugh randomly at any moment day or night (inappropriate context).

We used a PD technique called *Line Judging* [91] to have the children assess the scenarios. *Line Judging* is an evaluation technique that allows the design team to assess positive and negative feelings. We drew a 3-meter line on the whiteboard; we wrote "CREEPY" on one end, "NOT CREEPY" on the other end, and in the middle, "NOT SURE." One of the researchers read the first scenario with a slide deck presentation. Once the children heard the scenario, they moved themselves in the position on the line of their opinion. The children then shared their opinions of the scenarios with the adults; children also had the option to change their position on the line if their opinions changed. The process was repeated with each new scenario. To enhance internal validity, we counterbalanced the scenarios in DS2 with what we believed were non-creepy examples (e.g., a cute stuffed cat toy). Children in DS2 also had reactions that differed from what we expected, indicating the children had their own independent opinions.

Design Session 3 (DS3, May 2018): Based on initial criteria we were developing from DS1 and DS2, we went through YouTube and Apple App Store and chose 10 diverse technologies to present to the children. Such technologies included various social robots (e.g., Anki Cozmo [5], Woobo [4], Pepper the humanoid robot [2], Luvabella [6]), Internet of Things devices (e.g., toothbrush [9], water bottle [8], Google Clips video camera [3], Amazon Alexa Kids Edition [7]), diary smartphone apps (Maslo [10]), and headsets that could monitor emotion (Emotiv [1]). We implemented *Line Judging* [91] again, using the same "CREEPY," "NOT CREEPY," and "NOT SURE" positions.

Design Session 4 (DS4, July 2018): Our aim was to triangulate data from DS1-3. We used a combination of *Big Props* [91] and *Bags of Stuff* [27] PD techniques. *Big Props* is a form of scenario-based design [76] in which design groups use large items to act out a scenario. We gave groups of three to four children and adults plastic bins and asked them to use *Bags of Stuff* [27] materials to design technologies that were trustworthy. Children and adult groups needed to act out a technological scenario with the plastic bins that showed how their designs evoked trust in users.

Interviews (August 2018): Finally, to confirm our findings, we interviewed eight of the eleven children (three of the children aged out of the team by Summer 2018) that participated in KidsTeam UW. We asked questions such as, "What makes technology creepy?", "Do you use technologies in your life you think are creepy?", and "Do your parents use technologies in their lives that are creepy to you?". We audio recorded and transcribed all interviews.

Data Analysis

We approached this analysis using grounded, inductive, and qualitative methods [23, 25]. The first and last authors of this study first examined the literature to see whether creepy themes were present in child-computer interaction. With little to go by in the literature, we generated the initial themes from DS1-4 through initially open discussions of the video data. Next, we began an inductive analysis of a total of 297 minutes of video data (not including snack time). Primary and secondary reviewers (co-authors, not first/last authors) watched the videos and transcribed the entire DS1-4. For DS1 and 4, because the camera moved throughout the design sessions to focus on specific groups, we transcribed the individual conversations and the group discussion. For DS2 and 3, we transcribed only the conversations around the scenarios and technologies and the larger group discussions.

Once transcriptions were completed, we partitioned the transcript into individual child utterances that could be categorized. We analyzed the data using affinity diagramming, a method for organizing large amounts of qualitative data [44]. Affinity diagramming is an inductive approach that iteratively defined, refined, and combined the statements (notes) into larger themes. Our group constructed our affinity diagram through *RealtimeBoard*, an online collaborative whiteboard that allowed us to work together remotely to generate themes [11]. We visually represented each statement from a child pertaining to creepy technologies, fear, and motivations as a digital note. At times, children in this study used the terms "scary" and "creepy" interchangeably and struggled to articulate the distinction precisely. To denote the difference, we examined if the terms were centered around the ambiguity and uncertainty of fear. Thus, when children used the term "scary" to describe ambiguous threats, we denoted this instance as "creepy."

The authors of this paper iteratively organized the notes into themes over the course of four group discussions. We

used the individual child interviews as a way to triangulate the groups in DS1-4. This approach allowed us to complement themes generated by the group as a whole with children's individual perspectives. Overall, we identified eight major themes (two fears, five signals of creepiness, and one mediation).

4 FINDINGS

The children in our study reported several types of fear [43] in relation to their perceptions of technology. The two types we observed from our analysis were (1) *Physical Harm* and (2) *Loss of Attachment.* These two types of fears lay the foundation for how children describe the properties of technology they find creepy. We report on five design properties that prompt these fears and why they elicit these fear reactions: (3) *Deception vs. Transparency*, (4) *Ominous Physical Appearance*, (5) *Lack of Control*, (6) *Unpredictability*, and (7) *Mimicry.* Although we describe each of these as individual themes, we also found that they are interrelated and can compound one another's effects. Finally, we examine how children make sense of these fears and design properties through their (8) *Parents.*

The Fears that Technology Can Cause

Although a large body of work reports on threats children fear from technology, particularly with respect to surveillance and online safety [36, 51, 55, 94, 100], we found that children were more concerned with threats of physical harm and loss of attachment.

Physical Harm. At the most primal level, this type of fear refers to physical and bodily harm (whether real or imagined) that could occur as a result of a technological innovation [43]. Children in this study often used words such as "*kill*," "*murder*," and "*dead*" to convey their fears about creepy technologies. We asked the children in interviews to draw creepy technologies. All of them independently drew some form of monstrous technologies [82], ready to take over their lives and physically harm them (e.g., "*kill me*"). As such, children frequently mentioned a fear of technologies stalking them. They depicted stalking (whether by technology or by a person using technology) as a form of dreadful waiting in advance of physical harm. In this context, children explained there was a difference between things that are "scary" and things that are "creepy." Daniel summed up this distinction saying (DS2), "*Creepy is a long-term, and scary is a short term.*" In this case, creepy stalking is persistent, always in the background, and waiting to cause harm. Alejandro explained (DS2) that surveillance in technology was creepy because, "*you basically just feel like he [the technology] is waiting for the moment to kill you.*"

Children also described physical harm from creepy technologies as a form of punishment. In DS1, Justice and Daniel built a creepy stalking suit that would electrocute the user at random for punishment. Another type of physical fear came in the technology's size and shape. In DS3, Grace thought the child-sized Pepper robot was frightening because it was large enough to push her around. Grace expressed, "*I am so scared [of Pepper the robot]. If it is this big [put her hands on her head to indicate the height], I am scared. Because, because it [can] literally like smash everything.*"

Loss of Attachment. Children in this study frequently explained that creepy technologies scared them because they feared they might take them away from their parents. Grace stated (Interview) that creepy technologies can take you away from your mom and dad, where she felt safety. However, children expressed their concerns about the loss of attachment relationships as more than just the loss of protection from physical harm. Children in this study frequently referred to the animation movie, *Coraline* [46] (DS1, interviews - Grace, Sushi). In the movie, the protagonist (Coraline) travels to a parallel world, where she meets dolls that act like her parents. The parent dolls treat Coraline well and ask her to stay in their world, on the condition they sew buttons over Coraline's eyes.

The plotline of *Coraline* [46] mirrors some of the technological fears that children expressed related to loss of attachment. First, children frequently used the phrase, "*taking over your life*" to describe creepy technologies. Maggie said (Interview), "*Because if it [a creepy technology] was in your life, and it was trying to take over your life, then I would die.*" And children were particularly preoccupied with the idea that a technology might try to act like their parents. Alejandro (Interview) noted that it would be fine if digital voice technologies mimicked Barack Obama, but that it would not be okay if the technologies sounded like his parents. This fear is not unheard of; researchers have been able to accurately synthesize Barack Obama's voice using neural networks [85].

Similarly, as technologies advance, children explained that it seemed creepy to not be able to distinguish between loved ones and digital technologies. Polly showed concern in DS2, "*Cause it [a Roomba with voice] can replicate your parent's voice and make you believe it's your parents. And it's not trusting your parents that it's actually your parents.*" And when children mentioned their fears related to stalking, they explained that they feared technology was stalking to learn how to become like their families. Vice versa, if technology could act as a parent, it could also mimic a child, thereby leaving open the threat of taking the child's place. Sushi noted (DS3), "*What if, what if they [parents] ignore me. What if, what if they [parents] want Pepper [robot] and not me?*"

The Design Properties of Creepiness

Children consistently surfaced five properties that signal creepiness in technologies, which we describe in the subsections below.

Deception vs. Transparency. Children frequently described creepy technologies as ones that deliberately and intentionally try to deceive users by cultivating false mental models of interactions or outcomes. For instance, children considered it creepy if a technology did not intentionally give enough information for them to fully understand it. In DS2, Akane described a creepy scenario in which a Roomba vacuum cleaner called out their names using their parent's voice.

> Akane: *Because, um, because it's like, this is actually Roomba talking, like, if your parents recorded that [message], I don't think they would say, "This is actually Roomba talking." I think they would say, "This is, like, this is a recording or something."*

In Akane's description, the technology did not actively declare who was speaking, so it appeared the technology was trying to deceive the child into believing a parent was speaking.

Similarly, children thought about deception with respect to the way others might use a technology. They described creepy technologies as conduits through which strangers might interact with them. Such interactions included hacking, theft, secret recordings, and stalking. However, children noted that surveillance via technology did not concern them or feel deceptive when it came to their own parents. Children in this study welcomed parental monitoring, so long as it was made transparent that the technology was sending pertinent information directly to parents. For instance, children were comfortable with the idea of using a smart water bottle that would monitor their water intake and share this information with parents (DS3).

Children in this study asked for more transparency from designers in helping them understand how the technology works and whether it is trustworthy.

> Daniel: (Interview) *Like I'll say - call Jan Smith [mom, pseudonym] and it [digital voice assistant] will call that person. Okay, it will call them. Then when I ask - will you kill me in my sleep? It says - I can't answer that.*

Here, Daniel wanted a direct "*no*" in answer to his questions about killing him while he slept. Children noted that broad, non-specific answers to difficult questions made the technology appear creepy because they projected ambiguity. Researchers have noted that intelligent user interfaces cannot just provide simple "I don't know" or "I'm not sure" responses to children when asked difficult questions [95]; here, we shed light on one reason why.

Ominous Physical Appearance. How technology looks, sounds, and feels is often an initial signal of creepiness. For children in this study, the physical appearance was very influential in their opinions about a technology and its creepiness. Children expressed an expectation for what was "cute" and what was "scary" looking. For instance, using the K-2SO robot toy (Figure 1a) in DS2 consistently generated strong vehement responses from the children as creepy. Children thought, K-2SO's black and cold appearance looked like it was "*staring at you*" and "*waiting for him to kill you.*"

Ominous physical appearances did not have to be intentional. For instance, children thought the Pepper humanoid robot (DS3, Figure 1c, [2]) was creepy looking because it was missing legs, was tall, and had eyes that resembled a camera. In contrast, children leaned towards technologies that were cute. The children did not like Maslo (DS3, Figure 1g, [10]), an app with a large, black dot, because it looked like a, "*black spirit*" and a "*black hole.*" In contrast, children described Pusheen's appearance (DS2, Figure 1b) as, "*potatoes in the ears and the face,*" "*fat,*" "*cute,*" and "*friendly.*" Anki Cozmo (DS3, Figure 1d, [5]), compared to Pepper robot (Figure 1c, [2]), was "*tiny*" and "*acted stupid,*" indicating that it was not threatening. However, children also noted that physical appearances can also be deceptive when it comes to creepy technologies. Both Daniel and Akane noted that if technology was "*too cute,*" it could be hiding something sinister.

Interestingly, even if a technology included components that might raise privacy or surveillance concerns, if the design was cute looking, children looked past such issues. In DS3, children in the study overwhelmingly wanted to own a Woobo (Figure 1e, [4]), a social robot toy with an embedded microphone, Internet connectivity, and messaging application, because it, "*looks so cute.*" In contrast to Woobo in DS3, children disapproved of Luvabella (Figure 1f, [6]), a robotic human doll that suggests the uncanny valley [68, 69]. In this case, although a humanoid doll might appear harmless, children stated that the doll's laughter, eye blinking, and movements suggested it had ulterior motives. Similarly, Daniel noted (DS3), "*That is even more creepy because it's cuter. If it's cuter and doing creepy things, it's worse.*"

Lack of Control. Children frequently expressed concerns about lacking the ability to control the technology, its actions, or outputs (e.g., information, security). Children explained that lacking control over a technology contributed to their sense of it being creepy. They explained that in part, this stems from the fact that technology appears more "*alive*" and has more agency, which they find disturbing.

> Kenshin: (Interview) *Yeah, so, it's like Alexa is in this room and she starts interrupting this conversation... Or like she actually had a brain.*

For children, as technology gets out of their control, it seems more alive and deceptive.

A lack of control over technology is also indicative of controlling the flow of information to others (e.g., parents, strangers, etc.). First, the children wanted to control access of information to the technology. For instance, in DS4, Daniel and Raymond built an intelligent trashcan that let children know it both scanned and deleted their facial recognition data each time. The children also put a button on the trashcan that allowed for manual deletion of data. Alejandro (Interview) noted that the iPod Touch we were using for audio recordings was not creepy "*because then you can like delete what it said or like do stuff.*" Similarly, Alejandro stated that smartphone gaming apps were not creepy, because he felt he had full control over when to turn them on, when to turn them off, and when to delete them. As long as he felt he was in control of when an app was on, Alejandro did not consider gaming apps creepy. However, for children (and even adults), this may be a false sense of security, as many of these experiences may be conducting more surveillance than users realize.

Second, children wanted to control the flow of information to their parents. Polly jokingly expressed (DS2), "*Yeah it is like, it [the technology] comes at your parents and goes like, 'You should stop feeding your kids candies.' That is like my worst nightmare!*" Polly does note the extent to which children want their information shared and surveilled by technology. In her case, this is about technology trying to manipulate her parents and in some way intrudes on her relationship with them.

Unpredictability. Children also said that objects that typically seem benign become sinister when they hint that their behavior may be different from what children expect. Kenshin described (DS2) this kind of paradigm shift in his perception of an Amazon Echo voice assistant saying, "*Because then it would be a model of a person except it was like, an Amazon or an Alexa or Google and it talks exactly like a human... So, it wouldn't like only respond to when you say 'Alexa' or 'Hey, Google.'*" In this case, he explains that the digital voice assistant with which he is familiar becomes creepy when its predictable response pattern shifts.

Furthermore, the perception of creepiness becomes more apparent when these unpredictable behaviors are also contextually inappropriate. For instance, the children thought laughter from technology in response to a joke was disconcerting.

> Grace: (DS2) *When it [the technology] laughs at your joke or it responds, it's sort of creepy because, like, if it's like my mom or dad or my friend or my teacher, not creepy.*

Grace's existing paradigm maintains that a technology cannot understand jokes; laughter from a device in response to a joke signals that this is not a paradigm upon which she can rely. Laughing has multiple purposes, one of which is to communicate malintent. Akane noted in DS2, "*But, with the laughing, it's like a creepy murderer coming into my house.*" Grace expressed (DS2), "*It's so much creepier because it seems like someone's laughing to kill you... Like if, when people laugh at night, it makes me so scared.*" In this case, the random laughter at night amplifies an already fearful time for children (bedtime).

In complete contrast, we asked the children if it would be fine if technology made flatulence sounds ("*if the technology farted?*"). For the children, technology farting was completely fine and not creepy (Polly in DS2: "*farting is adorable*"). To the children, laughter from the technology is a form of speaking and can communicate many intents, from benevolent to threatening. Daniel explained (DS2), "*It's [laughter is] like speaking. It's like physically speaking, but [farting] - you're not actually making noise [to communicate] and ... [laughter is] like speaking, but it's not speaking.*" Daniel indicated a subtle and important distinction: laughter can be motivated by multiple intents, but farting lacks this motivational nuance. Flatulence is a random sound with a lack of malintent, but indicates toilet humor and embarrassment [70]. In contrast to laughing, farting at night is fine (Grace in DS2: "*it's basically normal during the day or night*") because it is contextually appropriate.

Mimicry. We refer to mimicry as technology pretending and imitating as something else. Similar to the uncanny valley [68, 69], children did not want technology to fully mimic humans and animals, but for different reasons than have been reported, generally in the space of human-robot interactions [20]. First, children had a visceral reaction to the idea of technologies trying to mimic the children themselves (*Me*). In DS2, many of them referred to this form of mimicry as a form of surveillance (Justice, Polly), a theft of their identity (Akane, Daniel), and a completely inappropriate use of technology (Grace). In particular, Grace had the most extreme reaction in DS3. She displayed jealousy when she realized Pepper the robot was child-sized, "*Yeah! It's like Pepper is here everybody, and then turns into ME, and then everybody just likes him.*" Children also described listening and stalking as mechanisms by which technology might try to mimic them and ultimately subsume their identity and personhood:

> Polly: (DS3) *Cause it - he's [technology] listening - you tell him, you tell the thing about your day and it just listens to you like, ohh, you tell it - it wants to take away your life!*

The fear of technology listening, becoming more intelligent, and taking over is not unusual; old stories and myths throughout different cultures show humans creating machines, but the machines (automata) turning against man

[62]. However, children anticipated extreme forms of intelligent intrusion, explaining, that as surveillance increased, technology could understand, for example, your feelings, know your blood type, understand inner thoughts, learn your humor and jokes, and figure out your actions. The children in this study called this, "*stealing your identity*" and taking away family attachments. This differs from how an adult might think about identity theft, which might be more focused on financial detriment by a stranger.

Second, similar to the loss of self, children thought technology wanting to mimic and act as their parents (or other people in their network) was creepy. For instance, children built a digital voice assistant that would attempt to steal their parents' identities and act like their parents (DS1). In DS2, we asked the children what they thought of a Roomba vacuum robot using their parents' voices to call to them. This idea of technology acting as their parents was disconcerting to the children.

Third, technology that mimics other humans inspired reactions in children that aligned with the uncanny valley perception [20, 68, 69]. Sushi strongly disliked Pepper the humanoid robot: "*It makes me feel like it's trying to be a child but it's not really a child... It makes me feel a bit creeped out! But it's cuz like, 'I am a child... a human robot'.*" In contrast, children had no misgivings about technology copying animals. The children thought it would be cute to hear technology purr like a cat or follow them like a pet. However, if the technology following and acting as an animal was seen as deceptive, then the children thought it was creepy.

Trust in Parents for Technologies

We asked in the interviews whether or not children thought their parents used creepy technologies. Children in this study trusted their parents' views on technologies in the home. For instance, Alejandro (Interview) relied on his mom's judgment, saying, "*If another person designed it [the technology] and my mom would be okay with it. That would be fine [for me].*" In Lily's interview, she noted that she trusted the technology in her home, because she trusted how her parents passed information to the technology.

> Lily: (Interview) *I'm not quite sure but I trust them [the technology] because I know that it's like [the technology] can't do anything with the information or anything like that.*

For Lily, she noted that the only way technology can gain access to information is when her parents give up that information (voice) to Siri. Here, she trusts that her parents have control over the information, therefore, the technology in their home must be safe. In general, most of the children explained their parents do not use creepy technologies. Maggie explained, "*Well, [my parents use] computer, iPads, TV, yep.*" We asked if those technologies were creepy, and
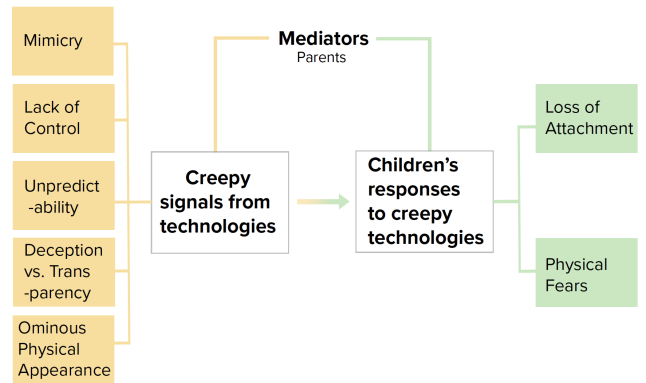

Figure 2: A conceptual model of children's perceptions of creepy technologies.

Maggie replied simply, "*No*". Interestingly, consumer technologies like smartphones, laptops, and tablets have some of the creepy design properties they mentioned (i.e., deception and transparency, lack of control). But some of the children did not see them as creepy, since their parents frequently used them in the home.

In contrast, Raymond's family placed covers on laptop video cameras to prevent unwanted surveillance ("*So, the camera wouldn't be watching us [my family]*"). We asked why he thought his parents did this. He explained (Interview), "*like it [home technology] could do something and it could watch you and stuff do something or go somewhere.*" People that could watch you were "*robbers*" and "*hackers*" that would find a way to change your passwords. In this case, Raymond's negative perceptions of creepiness are mediated by his parents' actions toward preventative measures.

5 DISCUSSION

Modeling Creepiness

Based on our themes, we developed a conceptual model. Figure 2 visualizes the major themes and subthemes.

Signals. Throughout our design sessions, children surfaced a recurring set of properties that signal to them that a technology felt creepy. *Deception and transparency*, an *ominous visual appearance*, *lack of control*, *mimicry*, and *unpredictability* each raised concerns for the children in our study. The children reported that an Amazon Echo could be creepy if it was *deceptive* (e.g., if a stranger hacked the device to listen in), took *control* (e.g., if children could not choose when the device could listen), was *unpredictable* (e.g., gave responses that were contextually inappropriate), or engaged in *mimicry* (e.g., if the device developed a mind). Individually and collectively, these cues from technology trigger for children the possibility that the technology poses a threat, a state known as fearful arousal [81].

Fears. Similarly, children raised two recurring concerns about the risks from creepy technologies, explaining first that the technology might pose a threat to their *physical safety*. Second, children repeatedly surfaced scenarios in which a technology has the potential to intrude on or even dismantle their *trusted network and attachment relationships* (most often parents). Robots that were too large became physically threatening, and while children were comfortable with a computer voice pretending to be Barack Obama, they were terrified of the idea of the same interface pretending to be their parent. Creepy signals from a technology can lead children to evaluate it in light of these concerns, thus we model these signals as predictive antecedents to two deep-seated fears (Figure 2).

Mediation. However, participants also made clear that the relationship between signals and fears is mediated by parents' input. Children explained that they look to trusted adults as proxies for detecting creepy or otherwise untrustworthy technologies. Parents mediate the relationship between creepy signals from a technology and children's assessment. That is, when an adult they trust deems a technology trustworthy, children accept this assessment and transitively extend their trust to the system. When adults describe a technology as creepy, it becomes more alarming to children, similar to vicarious learning of fear [12–14].

This model expands prior work documenting the technologies adults find concerning [16, 18, 36, 45, 58, 84, 94, 100], and other work documenting children's fears [20, 30, 42, 43, 71, 72, 79]. Here, we narrow the set of considerations to those that were relevant for the 7-to-11-year-olds in our study and examine the way in which design decisions align with the fears surfaced by children.

The Utility of the Model

Our model suggests designers have a responsibility to reflect on how they might trigger childhood fears. Childhood fears can be pervasive and last into adulthood as phobias [74], and acute events that first instill these fears (e.g., viewing a horror movie) can shape an individual's behavior for decades [22]. Our findings suggest that today, designers may not always incorporate these concerns into their process, and as a result, some create smart speakers that are baffled by the question, "*Will you kill me in my sleep?*" rather than ones that are prepared to address it and are sensitive to its importance. While it is difficult for designers to anticipate all types of creepy concerns, we believe intentional and explicit attempts to mitigate the creepy perception in children is still worthwhile. The fears that did not surface in these conversations are also noteworthy. Children failed to mention many crucial privacy and security concerns that are pervasive in both public discourse and computing scholarship, such as financial identity theft, targeted advertisements, or data mining. At

times researchers asked leading questions about surveillance technologies or data collection, but children did not latch on to these concerns.

This distinction is consistent with prior work suggesting a gap in children's awareness of these technology risks [55, 56, 64, 94, 100]. And more interestingly, it also suggests a gap between designers' and researchers' conceptions of technology risks and the concerns that are actually most salient for younger users. Children in our study looked to the visual interface and other overt signals for signs of concern, rarely mentioning what might be going on behind the scenes. Thus, our model not only highlights the importance of designing against unproductive fear, it also questions whether interfaces are currently too effective in suppressing children's fear responses. For example, what should we make of the fact that cuddly Woobo [4] raised no red flags for children in this study, even though it has some potential for risk with an embedded microphone, Internet connectivity, and data collection?

Implications for Parents and Designers

Our conceptual model of creepiness can support families and designers. From our model, we derived a set of questions that both families and designers can use to better understand children's perspectives of creepiness in technologies.

- *Deception*: What information is okay for people to know about children? Who do we think is trustworthy? Do we think technology could deceive people? Why and how?
- *Ominous Physical Appearance*: What do we want a technology to look like? Do technologies that look and feel nice always act nice?
- *Lack of Control*: How much control do children have over technologies? What kind of information should children be able to have control over?
- *Mimicry*: What do we think about our relationship with technology? Could technology ever replace people?
- *Unpredictability*: What are appropriate ways technology should act with people?
- *Relationships*: What do you think about parent/guardian usage of technology? How does technology usage in parents affect children's views of that relationship?

Family Implications. Studies of HCI in family contexts recommend shared conversations between parents and children around issues of monitoring, privacy, media use, and fear [36, 56, 65, 94]. Our research supports such conversations and demonstrates the importance of parents' perceptions of the trustworthiness of technology, at least for the children we worked with. Our findings complement Kumar

et al.'s [56] recommendations on parental scaffolding of privacy and security for children. Children relied on their parents' assessment of the creepiness of technology as a way to gauge their own understanding, and they reported that they trusted (to some extent) many common technologies, such as tablets and smartphones, because their parents use them. These findings and questions can provide a scaffolded way in which parents can have discussions together with children about their collective fears or concerns with respect to a particular technology.

Designer Implications. This framework and questions also provide guidance to designers seeking to create technologies children deem trustworthy and technologies that are, in fact, worthy of their trust. For example, a heuristic evaluation [73] conducted together with children could walk through a list of signals that potentially raise concerns, asking questions like, "*Can you imagine this technology lying to you?*" (Deception), or "*What are some things this technology might be able to do that you might not like, and how would you stop it from doing those things?*" (Control).

Similarly, designers might also conduct an analysis of potential risks their system poses to children and evaluate the extent to which their interface creates a false sense of security in light of these risks. We propose that the extent to which a UI works to build trust with a child should be commensurate with the trustworthiness of the system behind it and the risk to which the child is exposed. For example, a friendly character with whom a child is likely to develop a para-social relationship should be the face of a system that has an equally trustworthy back-end. Consistent with prior work (e.g., [65, 88]), we advocate for more transparency in technologies for children.

Further, our findings suggest front-end appeal and back-end trustworthiness are not always aligned. For example, children in this study believed that smartphones were not creepy and that when a user closes an app, all access to information will cease. However, this is not the case for many apps [54, 57], suggesting children (and adults) may have a false sense of security with respect to common technologies. We advocate for systems to embed in their front-end components a more realistic presentation of the risks they pose. Currently, technologies geared at ages 13 and older (e.g., Facebook, Google, Apple) are attempting to design towards more user-friendly privacy notices and controls [80]. However, the same trend also needs to happen towards children's technologies.

Ethical Considerations

In this study, we outline design properties that can be manipulated to signal to a child that a system is concerning. We believe this raises an ethical dilemma, as it has the potential to support nefarious actors seeking to suppress children's

fear responses to problematic technologies. For example, a social robot with charming visual appeal could give children a false sense of control (e.g., shutting it off does not mean it is actually off). *Dark Patterns* are pervasive design patterns that exploit users for the benefit of the developer [33, 99], and it is possible that documenting the design features children find creepy would support such work. At the same time, we believe this conceptual model also can arm parents, children, advocacy groups, and ethical designers with knowledge of what to look for, how to think critically about technologies, and develop new conversations about creepiness, fear, threat, and safety. We also believe that it will be up to the HCI community to examine designs for children, both from the perspective of adults and children, to gauge creepiness and potential for threat.

Limitations and Future Work

We developed our model through design sessions with 11 children in a single geographic region, all of whom have extensive experience with technology and design. Therefore, we contribute to formative theoretical generalizations in this space [96], not statistical generalizations [97]. Future work remains to examine how robust these themes are more widely seen. The children in this study also know each other well (e.g., friends, siblings) through extended co-design work. As a positive factor, children were not afraid of informing us of their fears. They were comfortable riffing off of each other (and the adults), working together, and disagreeing with each other in all the design sessions. At times, the children were distracted by their close relationships. Their close relationship also makes it more likely that their comments reflect the culture of the specific group.

We also conducted this work with children alone, and future co-design sessions that incorporate parents could expand this work to a whole-family perspective. Future surveys, usability studies, or experimental studies could evaluate the prevalence and validity of the themes we encountered to validate and expand on our model [96]. Additional work remains to iteratively develop prompts for parents and for designers to reflect on interfaces and designs in light of the risks they pose and the fears they inspire. This work can also go deeper to specific technologies, such as virtual and augmented reality, and mobile technologies, to understand specificities in design that are creepy.

6 CONCLUSION

Across the four design sessions and corroborated by individual interviews, we saw two basic fears of technologies and five consistent themes in the design properties that children find creepy, including concerns about a technology's visual appearance, control, unpredictability, ability to mimic others, and likelihood of deceiving the user. By working closely

with children with PD methods, we were able to generate deeper understandings of the relationship between creepy signals and fearful responses in children. These signals that a technology is creepy raise two specific fears for children, namely, that their physical safety might be at risk, or that the technology will intrude on or disrupt their relationship with a parent or other trusted adult.

Much of the research in HCI on security and privacy for children and families has focused on parental fears around technologies [16, 18, 36, 94, 100] and strategies to protect children [24, 55, 58, 59, 66]. Our findings illuminate core fears of children that are overlooked in the design process and have the potential to be invoked by technology. We argue that it is essential to understand more deeply children's fears of technology and how they make sense of the digital world around them. While we do not believe it is possible (or wise) to eliminate all potential childhood fears in technology, we do believe that understanding children's perceptions in this manner helps us to develop new designs and methods to support resilience in children, transparency in design, and security with families.

ACKNOWLEDGMENTS

REFERENCES

[1] 2014. Emotiv's new neuro-headset. Retrieved 2018-09-18 from https://www.youtube.com/watch?v=bposG6XHXvU

[2] 2014. Meet Pepper, the friendly humanoid robot. Retrieved 2018-09-18 from https://www.youtube.com/watch?v=lqlyxg1-gE0

[3] 2017. Google Clips: AI camera first look. Retrieved 2018-09-18 from https://www.youtube.com/watch?v=w05jWoaIHUs

[4] 2017. Meet Woobo on Kickstarter! Retrieved 2018-09-18 from https://www.youtube.com/watch?v=Z_ip6nigzDg

[5] 2017. MY NEW PET ROBOT!!! Hanging out with COZMO! Robot companion from Anki. Retrieved 2018-09-18 from https://www.youtube.com/watch?v=0P_nAxFOB10

[6] 2017. Toy Fair 2017: LuvaBella doll from Spin Master. Retrieved 2018-12-23 from https://www.youtube.com/watch?v=8CJH5IYD5hY

[7] 2018. Echo Dot Kids Edition. Retrieved 2018-09-18 from https://www.youtube.com/watch?v=jNdZAgij-K0

[8] 2018. Gululu Interactive Bottle. Retrieved 2018-09-18 from https://www.youtube.com/watch?v=_Lnd9Mx2e3E

[9] 2018. Kolibree's Magik AR toothbrush makes brushing a game. Retrieved 2018-09-18 from https://www.youtube.com/watch?v=2MlQRR81r9c

[10] 2018. Maslo. Retrieved 2018-09-18 from https://itunes.apple.com/us/app/maslo/id1330018942?mt=8

[11] 2018. RealtimeBoard. https://realtimeboard.com/

[12] Chris Askew, Gijler Dunne, Zehra Üzdil, Gemma Reynolds, and Andy P. Field. 2013. Stimulus fear-relevance and the vicarious learning pathway to childhood fears. *Emotion* 13, 5 (2013), 915–925. https://doi.org/10.1037/a0032714

[13] Chris Askew and Andy P. Field. 2007. Vicarious learning and the development of fears in childhood. *Behaviour Research and Therapy* 45, 11 (Nov. 2007), 2616–2627. https://doi.org/10.1016/j.brat.2007.06.008

[14] Chris Askew, Gemma Reynolds, Sarah Fielding-Smith, and Andy P. Field. 2016. Inhibition of vicariously learned fear in children using positive modeling and prior exposure. *Journal of Abnormal Psychology* 125, 2 (Feb. 2016), 279–291. https://doi.org/10.1037/abn0000131

[15] Brigid Barron, Caitlin Kennedy Martin, Lori Takeuchi, and Rachel Fithian. 2009. Parents as learning partners in the development of technological fluency. *International Journal of Learning and Media* 1, 2 (May 2009), 55–77. https://doi.org/10.1162/ijlm.2009.0021

[16] Lindsay Blackwell, Emma Gardiner, and Sarita Schoenebeck. 2016. Managing expectations: Technology tensions among parents and teens. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. ACM Press, New York, NY, 1390–1401. https://doi.org/10.1145/2818048.2819928

[17] Isabelle Blanchette. 2006. Snakes, spiders, guns, and syringes: How specific are evolutionary constraints on the detection of threatening stimuli? *The Quarterly Journal of Experimental Psychology* 59, 8 (August 2006), 1484–1504. https://doi.org/10.1080/02724980543000204

[18] danah boyd and Eszter Hargittai. 2013. Connected and concerned: Variation in parents' online safety concerns. *Policy & Internet* 5, 3 (Oct. 2013), 245–269. https://doi.org/10.1002/1944-2866.POI332

[19] Pascal Boyer and Brian Bergstrom. 2011. Threat-detection in child development: An evolutionary perspective. *Neuroscience & Biobehavioral Reviews* 35, 4 (March 2011), 1034–1041. https://doi.org/10.1016/j.neubiorev.2010.08.010

[20] Kimberly A. Brink, Kurt Gray, and Henry M. Wellman. 2017. Creepiness creeps in: Uncanny valley feelings are acquired in childhood. *Child Development* 0, 0 (December 2017). https://doi.org/10.1111/cdev.12999

[21] Rebecca J. Brooker, Kristin A. Buss, Kathryn Lemery-Chalfant, Nazan Aksan, Richard J. Davidson, and H. Hill Goldsmith. 2013. The development of stranger fear in infancy and toddlerhood: normative development, individual differences, antecedents, and outcomes. *Developmental Science* 16, 6 (Nov 2013), 864–878. https://doi.org/10.1111/desc.12058

[22] Joanne Cantor. 2004. "I'll never have a clown in my house" - Why movie horror lives on. *Poetics Today* 25, 2 (June 2004), 283–304. https://doi.org/10.1215/03335372-25-2-283

[23] Kathy Charmaz and Liska Belgrave. 2012. Qualitative interviewing and grounded theory analysis. In *The SAGE handbook of interview research: The complexity of the craft*. Vol. 2. Sage Thousand Oaks, CA, 347–365.

[24] Lynn Schofield Clark. 2011. Parental mediation theory for the digital age. *Communication Theory* 21, 4 (Oct 2011), 323–343. https://doi.org/10.1111/j.1468-2885.2011.01391.x

[25] John W. Creswell. 1998. *Qualitative inquiry and research design: Choosing among five traditions*. Sage, Thousand Oaks, CA.

[26] Irene H.A. De Goede, Susan J.T. Branje, and Wim H.J. Meeus. 2009. Developmental changes and gender differences in adolescents' perceptions of friendships. *Journal of Adolescence* 32, 5 (Oct 2009), 1105–1123. https://doi.org/10.1016/j.adolescence.2009.03.002

[27] Allison Druin. 1999. Cooperative inquiry: Developing new technologies for children With children. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, 592–599.

[28] Allison Druin. 2002. The role of children in the design of new technology. *Behaviour and Information Technology* 21, 1 (2002), 1–25. https://doi.org/10.1080/01449290210147484

[29] Allison Druin. 2005. What children can teach us: Developing digital libraries for children with children. *The Library Quarterly* 75, 1 (Jan

2005), 20–41. https://doi.org/10.1086/428691

[30] Kerry-Ann Egliston and Ronald M. Rapee. 2007. Inhibition of fear acquisition in toddlers following positive modelling by their mothers. *Behaviour Research and Therapy* 45, 8 (Aug 2007), 1871–1882. https://doi.org/10.1016/j.brat.2007.02.007

[31] Pelle Ehn. 2017. Scandinavian design: On participation and skill. In *Participatory design: Principles and practices*. CRC Press, 41–77.

[32] Andy P. Field, Sally J. Hamilton, Karina A. Knowles, and Emma L. Plews. 2003. Fear information and social phobic beliefs in children: a prospective paradigm and preliminary results. *Behaviour Research and Therapy* 41, 1 (Jan 2003), 113–123. https://doi.org/10.1016/S0005-7967(02)00050-5

[33] Brian J. Fogg. 2002. Persuasive technology: Using computers to change what we think and do. *Ubiquity* 5 (Dec 2002). https://doi.org/10.1145/764008.763957

[34] Rodrigo Franco, Roberto Sánchez-Olea, Elsa M. Reyes-Reyes, and Mihalis I. Panayiotidis. 2009. Environmental toxicity, oxidative stress and apoptosis: Ménage à trois. *Mutation Research/Genetic Toxicology and Environmental Mutagenesis* 674, 1-2 (March 2009), 3–22. https://doi.org/10.1016/j.mrgentox.2008.11.012

[35] Antje B.M. Gerdes, Gabriele Uhl, and Georg W. Alpers. 2009. Spiders are special: fear and disgust evoked by pictures of arthropods. *Evolution and Human Behavior* 30, 1 (January 2009), 66–73. https://doi.org/10.1016/j.evolhumbehav.2008.08.005

[36] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J. LaViola Jr., and Pamela J. Wisniewski. 2018. Safety vs. surveillance: What children have to say about mobile apps for parental control. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, 124:1–124:14. https://doi.org/10.1145/3173574.3173698

[37] Anne Grey et al. 2011. Cybersafety in early childhood education. *Australasian Journal of Early Childhood* 36, 2 (2011), 77–81.

[38] Lisa Guernsey. 2012. *Screen time: How electronic media from baby videos to educational software affects your young child*. Hachette UK.

[39] Lisa Guernsey and Carla Seal-Wanner. 2007. *Into the minds of babes: How screen time affects children from birth to age five*. Basic Books New York, NY.

[40] Mona Leigh Guha, Allison Druin, Gene Chipman, Jerry Alan Fails, Sante Simms, and Allison Farber. 2004. Mixing ideas: A new technique for working with young children as design partners. In *Proceedings of the 2004 Conference on Interaction Design and Children: Building a Community*. ACM, New York, NY, 35–42. https://doi.org/10.1145/1017833.1017838

[41] Mona Leigh Guha, Allison Druin, and Jerry Alan Fails. 2013. Cooperative Inquiry revisited: Reflections of the past and guidelines for the future of intergenerational co-design. *International Journal of Child-Computer Interaction* 1, 1 (Jan 2013), 14–23. https://doi.org/10.1016/j.ijcci.2012.08.003

[42] Eleonora Gullone. 1999. The assessment of normal fear in children and adolescents. *Clinical Child and Family Psychology Review* 2, 2 (July 1999), 91–106. https://doi.org/10.1023/A:1021895630678

[43] Eleonora Gullone. 2000. The development of normal fear. *Clinical Psychology Review* 20, 4 (June 2000), 429–451. https://doi.org/10.1016/S0272-7358(99)00034-3

[44] Gunnar Harboe and Elaine M. Huang. 2015. Real-world affinity diagramming practices: Bridging the paper-digital gap. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 95–104. https://doi.org/10.1145/2702123.2702561

[45] Heidi Hartikainen, Netta Iivari, and Marianne Kinnula. 2016. Should we design for control, trust or involvement?: A discourses survey about children's online safety. In *Proceedings of the The 15th International Conference on Interaction Design and Children*. ACM, New York, NY, 367–378. https://doi.org/10.1145/2930674.2930680

[46] IMDb. 2009. Coraline (2009). Retrieved 2018-09-18 from http://www.imdb.com/title/tt0327597/

[47] IMDb. 2016. Rogue One: A Star Wars story (2016). Retrieved 2018-09-18 from https://www.imdb.com/title/tt3748528/

[48] Cecilie Javo, John A. Rønning, and Sonja Heyerdahl. 2004. Childrearing in an indigenous Sami population in Norway: A cross-cultural comparison of parental attitudes and expectations. *Scandinavian Journal of Psychology* 45, 1 (2004), 67–78. https://doi.org/10.1111/j.1467-9450.2004.00380.x

[49] Peter H. Kahn Jr. and Stephen R. Kellert. 2002. *Children and Nature: Psychological, Sociocultural, and Evolutionary Investigations*. MIT Press. Google-Books-ID: RCjdKjI_qIcC.

[50] Lawrence H. Keeley. 1997. *War Before Civilization*. Oxford University Press, USA. Google-Books-ID: Q8MHKQrFeEEC.

[51] Peter Kelly. 2000. The dangerousness of youth-at-risk: The possibilities of surveillance and intervention in uncertain times. *Journal of A* 23, 4 (August 2000), 463–476. https://doi.org/10.1006/jado.2000.0331

[52] Finn Kensing and Jeanette Blomberg. 1998. Participatory design: Issues and concerns. *Computer Supported Cooperative Work (CSCW)* 7, 3-4 (1998), 167–185. https://doi.org/10.1023/A:1008689307411

[53] Christie Kodama, Beth St. Jean, Mega Subramaniam, and Natalie Greene Taylor. 2017. There's a creepy guy on the other end at Google!: Engaging middle school students in a drawing activity to elicit their mental models of Google. *Information Retrieval Journal* 20, 5 (2017), 403–432. https://doi.org/10.1007/s10791-017-9306-x

[54] Mehrdad Koohikamali and Dan J. Kim. 2016. Do mobile app providers try enough to protect users' privacy? - A content analysis of mobile app privacy policies. *International Conference Information Systems 2016 Special Interest Group on Big Data Proceedings* (2016).

[55] 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 ACM Hum.-Comput. Interact.* 1, CSCW (Dec. 2017), 64:1–64:21. https://doi.org/10.1145/3134699

[56] Priya Kumar, Jessica Vitak, Marshini Chetty, Tamara L. Clegg, Jonathan Yang, Brenna McNally, and Elizabeth Bonsignore. 2018. Co-designing online privacy-related games and stories with children. In *Proceedings of the 17th ACM Conference on Interaction Design and Children (IDC '18)*. ACM, New York, NY, USA, 67–79. https://doi.org/10.1145/3202185.3202735

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

[58] Sonia Livingstone and Ellen J. Helsper. 2008. Parental mediation of children's internet use. *Journal of Broadcasting & Electronic Media* 52, 4 (2008), 581–599. https://doi.org/10.1080/08838150802437396

[59] May O. Lwin, Andrea J.S. Stanaland, and Anthony D. Miyazaki. 2008. Protecting children's privacy online: How parental mediation strategies affect website safeguard effectiveness. *Journal of Retailing* 84, 2 (2008), 205–217. https://doi.org/10.1016/j.jretai.2008.04.004

[60] Helia Marreiros, Richard Gomer, Michael Vlassopoulos, and Mirco Tonin. 2015. Exploring user perceptions of online privacy disclosures. *In Proceedings IADIS International Conference WWW/Internet - ICWI 2015* (2015).

[61] Alice E. Marwick. 2008. To catch a predator? The MySpace moral panic. *First Monday* 13, 6 (June 2008). https://doi.org/10.5210/fm.

v13i6.2152

[62] Bruce Mazlish. 2000. The man-machine and artificial intelligence. In *Artificial Intelligence*, Ronald Chrisley and Sander Beeger (Eds.). Vol. 1. Taylor & Francis, 134–160.

[63] Francis T. McAndrew and Sara S. Koehnke. 2016. On the nature of creepiness. *New Ideas in Psychology* 43 (Dec. 2016), 10–15. https://doi.org/10.1016/j.newideapsych.2016.03.003

[64] Brenna McNally, Priya Kumar, Chelsea Hordatt, Matthew Louis Mauriello, Shalmali Naik, Leyla Norooz, Alazandra Shorter, Evan Golub, and Allison Druin. 2018. Co-designing mobile online safety applications with children. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*. ACM Press, Montreal QC, Canada, 1–9. https://doi.org/10.1145/3173574.3174097

[65] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys that listen: A study of parents, children, and internet-connected toys. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 5197–5207. https://doi.org/10.1145/3025453.3025735

[66] Gustavo S. Mesch. 2009. Parental mediation, online activities, and cyberbullying. *CyberPsychology & Behavior* 12, 4 (2009), 387–393. https://doi.org/10.1089/cpb.2009.0068

[67] Robert S. Moore, Melissa L. Moore, Kevin J. Shanahan, and Britney Mack. 2015. Creepy marketing: Three dimensions of perceived excessive online privacy violation. *Marketing Management* 25, 1 (Jan 2015), 42–53.

[68] Masahiro Mori. 1970. The uncanny valley. *Energy* 7, 4 (1970), 33–35.

[69] Masahiro Mori, Karl F. MacDorman, and Norri Kageki. 2012. The uncanny valley [from the field]. *IEEE Robotics & Automation Magazine* 19, 2 (June 2012), 98–100. https://doi.org/10.1109/MRA.2012.2192811

[70] John Morreall. 2011. *Comic relief: A comprehensive philosophy of humor*. Vol. 27. John Wiley & Sons.

[71] Peter Muris, Pim Steerneman, Harald Merckelbach, and Cor Meesters. 1996. The role of parental fearfulness and modeling in children's fear. *Behaviour Research and Therapy* 34, 3 (1996), 265–268.

[72] Aisling Murray. 2012. What can children's fears tell us about childhood? An exploration of data collected as part of growing up in Ireland, The National Longitudinal Study of Children. *The Irish Psychologist* 38, 12 (Oct 2012).

[73] Jakob Nielsen and Rolf Molich. 1990. Heuristic evaluation of user interfaces. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '90)*. ACM, New York, NY, USA, 249–256. https://doi.org/10.1145/97243.97281

[74] Thomas H. Ollendick, Natoshia Raishevich, Thompson E. Davis III, Cristian Sirbu, and Lars-Goran Ost. 2010. Specific phobia in youth: Phenomenology and psychological characteristics. *Behavior Therapy* 41, 1 (March 2010), 133–141. https://doi.org/10.1016/j.beth.2009.02.002

[75] Chanda Phelan, Cliff Lampe, and Paul Resnick. 2016. It's creepy, but it doesn't bother me. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 5240–5251. https://doi.org/10.1145/2858036.2858381

[76] Mary Beth Rosson and John M. Carroll. 2003. Scenario-based design. In *The human-computer interaction handbook*, Julie A. Jacko and Andrew Sears (Eds.). L. Erlbaum Associates Inc., Hillsdale, NJ, USA, 1032–1050.

[77] Tanja Rothrauff, Wendy Middlemiss, and Lauren Jacobson. 2004. Comparison of American and Austrian infants' and toddlers' sleep habits: A retrospective, exploratory study. *North American Journal of Psychology* 6, 1 (2004), 125–144.

[78] Robert M. Sapolsky. 2004. Social status and health in humans and other animals. *Annu. Rev. Anthropol.* 33 (2004), 393–418.

[79] Sandra Scarr and Philip Salapatek. 1970. Patterns of fear development during infancy. *Merrill-Palmer Quarterly of Behavior and Development* 16, 1 (1970), 53–90.

[80] Florian Schaub, Rebecca Balebako, and Lorrie Faith Cranor. 2017. Designing effective privacy notices and controls. *IEEE Internet Computing* (June 2017), 1–1. https://doi.org/10.1109/MIC.2017.265102930

[81] Michelle R. Schuder and Karlen Lyons-Ruth. 2004. "Hidden trauma" in infancy: Attachment, fearful arousal, and early dysfunction of the stress response system. In *Young children and trauma: Intervention and treatment*. Guilford Press, New York, NY, US, 69–104.

[82] Tanya Sharon and Jacqueline D. Woolley. 2004. Do monsters dream? Young children's understanding of the fantasy/reality distinction. *British Journal of Developmental Psychology* 22, 2 (2004), 293–310. https://doi.org/10.1348/026151004323044627

[83] Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Hoskuldur Borgthorsson. 2014. Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2347–2356. https://doi.org/10.1145/2556288.2557421

[84] Peter N. Stearns. 2004. *Anxious parents: A history of modern childrearing in America*. NYU Press. Google-Books-ID: 8nkTCgAAQBAJ.

[85] Supasorn Suwajanakorn, Steven M. Seitz, and Ira Kemelmacher-Shlizerman. 2017. Synthesizing Obama: Learning lip sync from audio. *ACM Transactions on Graphics (TOG)* 36, 4 (2017), 95. https://doi.org/10.1145/3072959.3073640

[86] Lori Takeuchi, Reed Stevens, et al. 2011. *The new coviewing: Designing for learning through joint media engagement*. Technical Report. New York, NY: The Joan Ganz Cooney Center at Sesame Workshop.

[87] Lori M. Takeuchi and Michael H. Levine. 2014. Learning in a digital age: Toward a new ecology of human development. In *Media and the well-being of children and adolescents*, Amy Jordan and Daniel Romer (Eds.). Vol. 2. Oxford University Press Oxford, 20–43.

[88] Omer Tene and Jules Polonetsky. 2013. A theory of creepy: technology, privacy and shifting social norms. *Yale Journal of Law & Technology* 16, 1 (Jan 2013), 59–102.

[89] Gill Valentine and Sarah Holloway. 2001. On-line dangers?: Geographies of parents' fears for children's safety in cyberspace. *Professional Geographer* 53, 1 (Feb. 2001), 71–83. https://doi.org/10.1111/0033-0124.00270

[90] Patti M. Valkenburg, Marina Krcmar, Allerd L. Peeters, and Nies M. Marseille. 1999. Developing a scale to assess three styles of television mediation: "Instructive mediation", "restrictive mediation", and "social coviewing". *Journal of Broadcasting & Electronic Media* 43, 1 (1999), 52–66. https://doi.org/10.1080/08838159909364474

[91] Greg Walsh, Elizabeth Foss, Jason Yip, and Allison Druin. 2013. FACIT PD: A framework for analysis and creation of intergenerational techniques for participatory design. In *proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, 2893–2902. https://doi.org/10.1145/2470654.2481400

[92] Murray Weeks, Robert J. Coplan, and Adam Kingsbury. 2009. The correlates and consequences of early appearing social anxiety in young children. *Journal of Anxiety Disorders* 23, 7 (Oct 2009), 965–972. https://doi.org/10.1016/j.janxdis.2009.06.006

[93] Helen Westcott and Karen Littleton. 2005. *Exploring meaning through interviews with children*. Sage Publications Ltd, London, UK.

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

[95] Julia Woodward, Zari McFadden, Nicole Shiver, Amir Ben-hayon, Jason C. Yip, and Lisa Anthony. 2018. Using co-design to examine how children conceptualize intelligent interfaces. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA. https://doi.org/10.1145/3173574.3174149

[96] Robert K. Yin. 2013. Validity and generalization in future case study evaluations. *Evaluation* 19, 3 (2013), 321–332. https://doi.org/10.1177/1356389013497081

[97] Robert K. Yin. 2017. *Case study research and applications: Design and methods*. Sage publications, London, UK.

[98] Jason C. Yip, Kiley Sobel, Caroline Pitt, Kung Jin Lee, Sijin Chen, Kari Nasu, and Laura R. Pina. 2017. Examining adult-child interactions in intergenerational participatory design. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 5742–5754. https://doi.org/10.1145/3025453.3025787

[99] José P. Zagal, Staffan Bjork, and Chris Lewis. 2013. Dark patterns in the design of games. In *Foundations of Digital Games 2013*.

[100] Leah Zhang-Kennedy, Christine Mekhail, Yomna Abdelaziz, and Sonia Chiasson. 2016. From nosy little brothers to stranger-danger: Children and parents' perception of mobile threats. In *Proceedings of the The 15th International Conference on Interaction Design and Children - IDC '16*. ACM Press, Manchester, United Kingdom, 388–399. https://doi.org/10.1145/2930674.2930716