# From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats

**Leah Zhang-Kennedy**
Carleton University
Ottawa, Canada
leah.zhang@carleton.ca

**Christine Mekhail**
Carleton University
Ottawa, Canada
christine.mekhail@carleton.ca

**Yomna Abdelaziz**
Carleton University
Ottawa, Canada
yomna.abdelaziz@carleton.ca

**Sonia Chiasson**
Carleton University
Ottawa, Canada
chiasson@scs.carleton.ca

## ABSTRACT
The rise in mobile media use by children has heightened parents' concerns for their online safety. Through semi-structured interviews of parent-child dyads, we explore the perceived privacy and security threats faced by children aged seven to eleven along with the protection mechanisms employed. We identified four models of privacy held by children. Furthermore, we found that children's concerns fit into four child-adversary threat models: *child-peers, child-media, child-strangers, and child-parents*. Their concerns differed from the five threat models held by the parents: *child-peers, child-media, child-strangers, child-technology, and child-self*. Parents used a variety of protection strategies to minimize children's exposure to external threats. In reality, however, our results suggest that security and privacy risks from an internal family member or a friend are far more common than harm from outsiders.

### ACM Classification Keywords
H.5.m [Information Interfaces and Presentation]: Miscellaneous; H.1.2 [Models and Principles]: User/Machine Systems – *Human Factors*; K.8.3 [Personal Computing]: Management/Maintenance

### Author Keywords
Privacy; Threat Models; Usable Privacy and Security; Human Factors; Child-Computer Interaction; Mobile

## INTRODUCTION
The Internet is a rich educational tool for both adults and children alike, and it is shown to increase self-awareness and identity development in children [7, 9]. Children's online presence is facilitated by their orientation towards innovation and they are deemed to be more flexible and creative in their Internet use than their adult counterparts [9]. As Internet uses evolve, so too do the factors and implications around those interactions. Privacy and security issues become complex, and even more so when the users are children. Children's perceptions of privacy and security are less developed than those of adults. As a result, they often need to be protected from online threats [17, 18], particularly because of their naïve perception of online content and communication [14].

To design better privacy and security technologies for children, we studied the implications of privacy, security, and threats surrounding the use of mobile media by Canadian children aged seven to eleven years. Our current research consists of a qualitative comparative analysis of children and parents' perception of the threats and the protection strategies employed by these families. To fully understand children's perception of these topics, it is critical to include parents' perspective particularly because parents play an active role in children's daily interaction with mobile devices and they share the responsibility for managing children's privacy and security [1].

We explore three related research questions: R1) *Children's privacy*: How do children conceptualize privacy and what does 'being private' mean for children? R2) *Perceptions of potential threats*: How do children and parents' perceptions of threats surrounding mobile media differ from each other? R3) *Strategies to protect children*: How do parents protect their children from the perceived threats surrounding mobile media?

We draw from more than 35 hours of transcribed audio interviews with 14 families. Using Grounded Theory methodology [20], we identified four models of online privacy held by children. Our analysis suggest that the younger children's understanding of online privacy is 'to be alone' or 'to hide secrets or special things,' whereas older children had a more refined understanding. Furthermore, we identified four child-adversary threat models (*child-peers, child-media, child-strangers, and child-parents*) from the children and five child-adversary threat models (*child-peers, child-media, child-*



*IDC '16*, June 21-24, 2016, Manchester, United Kingdom

ACM 978-1-4503-4313-8/16/06.

http://dx.doi.org/10.1145/2930674.2930716

*strangers, child-technology, and child-self*) from the parents. We found large discrepancies in threat perceptions between the two groups. Children showed a very preliminary understanding of the harm caused, and perceived internal threats from siblings and parents to be more imminent than external threats from friends, strangers or online media. Parents on the other hand, were more worried about external threats. Parents used a variety of protection strategies to minimize children's exposure to external threats. In reality, however, our results suggest that security and privacy risks from a family member or a friend are far more common than harm caused by cybercriminals or outsiders. In fact, children and parents frequently put each other in risky situations that undermine their privacy and security.

## BACKGROUND

Mobile media is being introduced to children earlier than ever before; by age two, 38 percent of children had used smartphones [13]. Children's Internet use increases with age, and is diversifying across device types, with socio-economic status and gender appearing to affect the amount of Internet use [12]. In 2004, one large-scale survey [10] of 25,142 children across Europe found that 30 percent of the nine- to ten-year-olds spent time online on a daily basis. This figure rose to 80 percent of the fifteen- to sixteen-year-olds surveyed. This survey also covered the context of Internet use, finding that 87 percent reported to use the Internet at home and 63 percent at school. By 2014, the number rose significantly, with 99 percent of students from grades four to eleven having access to the Internet outside of school from a variety of portable platforms and devices [19]. In a related 2013 US study [13], around 72 percent of children aged 8 and under used a mobile device, and the average time children spend on mobile devices had tripled in two years. Children engaged in a variety of activities on their mobile devices, included playing games, watching video clips, instant messaging, posting images, and doing school work [10, 13, 19].

Factors affecting privacy and security can be subjectively defined and thus children's perceptions of their own privacy is important. Media Smarts [19] set a thorough example through a three-part series of child and teen-centred (grades four through eleven) study of online behaviours across a span of 14 years. Part one of the research suggested that young people value their online privacy. Part two found that they go online for social reasons and that parents exercise a variety of house rules to protect them against online risks. Part three included additional insights into children's and teen's online lives with recommendations for parents, teachers, and policy makers to help support young people growing up in the digital age. Hasebrink et al. [5] identified three classifications of risk to children online: content, contact, and conduct. The risk of content refers to children's exposure inappropriate online content; the risk of contact refers to being contacted by predators or users with malicious motivations; the risk of conduct has to do with the children themselves acting inappropriately or aggressively online.

Due to the potential risks inherent in online connectivity, children are frequently put under parental surveillance at home [11]. The Children's Online Privacy Protection Act (COPPA) in the U.S. [3] highlights that parents are seen as carrying the primary responsibility for supervising their children's Internet use. Parents feel a responsibility to protect their children from external harm, and from themselves due to their lack of maturity, experience, and the capacity for judgment required to make online decisions. Furthermore, the public's perception that 'parents are bad parents if they don't know where their children are and what they are doing at all times' puts social pressure on parents [24]. While parents have always supervised their children, it is uncertain whether the protection strategies that parents employ are in fact effective to protect children against threats posed by mobile technologies and the Internet.

Work in Usable Security [2, 4, 6, 22, 23] highlights that an important aspect of home security is users' existing knowledge about computer security issues and the technology they use. Users make decisions about security issues based on their existing 'folk models' [22]. They refer to how people perceive problems or concepts in ways that are not necessarily accurate or informed. Unfortunately, users typically rely on poor folk models with regards to technology and computer security that leads to erroneous decision making [22]. Little is known of young children's models of privacy and security and adults' models of surveillance technologies such as parental controls.

## METHODOLOGY

### Ethics and Recruitment

Our methodology was reviewed by the Carleton University Research Ethics Board-B. The participants were recruited through invitations shared with local community groups and personal acquaintances on Facebook and email in the cities of Ottawa, Kitchener-Waterloo, and Cambridge in the province of Ontario, Canada. Participation was limited to children aged seven to eleven and one child per family who used at least one mobile device on a regular basis. The adult participants were the parents or legal guardians of the child participants. The interviews typically took place at a public location of the parents' choice, such as at a community centre or a library. We obtained written consent from the adult participant followed by verbal informed assent from the child. Each parent and child was awarded a $10 gift card (a $20 honorarium per family).

### Participants and Procedure

We audio-recorded semi-structured interviews with 14 parent-child dyads. The children were between the ages of seven to eleven; eight were male (*Mean* age = 8.75) and six were female (*Mean* age = 8). Nine adult participants were between the ages of 31 and 40, five were between the ages of 41-50, and one was between the ages of 21 and 30. More mothers (11 participants) than fathers (3 participants) volunteered to accompany their child to the study. Four mothers were stay-at-home moms and the other parents had full time jobs in a variety of professions. Nine had a Bachelor's degree, four had a college diploma, one had a Masters degree, and another had a high school diploma.

All of the families had two or more children living in the household. The majority of children (12/14, 86%) lived with

two parents, while two children lived with a single mother. They all had Internet access at home and were regular users of mobile devices.

The parent-child dyads were briefed about the study together but interviewed separately. The adult participant completed a basic demographic questionnaire on gender, age, level of education, and occupation. A semi-structured interview followed with the adult participant, then with the child participant.

The interview questions were targeted to gain insight into children's use of mobile devices and their understanding of privacy related risks from two perspectives: from the point of view of the parent and from the perspective of the child. The interviews covered four main themes: General device use; Specific types of activities the child performs on the device; Who is responsible for maintaining the state of the device; The child's online privacy knowledge.

During the child interview, the parent was encouraged to be nearby but not sitting directly with the child to give the child more freedom to speak. However, we accommodated families who wished to sit together. If the child voluntarily disclosed sensitive personal information during the interview, it was removed from the transcription. Participants were not required to use any devices during the interview but some children voluntarily brought their devices to the study. At the end of each interview, the participants were debriefed and awarded their honorarium. Each dyad session took around one hour, approximately evenly split between the adult and child.

### Qualitative Data Analysis

We applied Grounded Theory methodology from Strauss & Cobin [20] for qualitative analysis as used in Human-Computer Interaction (HCI) research [8,15,16,21]. The aim of Grounded Theory is to create a set of well-developed concepts through the systematic analysis and the interpretation of empirical data [15]. The emergent theory is therefore grounded in the data. The methodology involves three major steps in the analysis process. The first step is *open coding* where the transcribed data is summarized point-by-point and descriptive codes are generated in an effort to discover coded properties and dimensions in the data. Since we initially organized the interview questions into four main themes, we began the analysis by coding instances of these themes in the order participants discussed them in the interview. During the process of *axial coding*, we systematically compiled the descriptive codes into themed categories and subcategories to uncover structure in the data and to identify the relationships between codes. In the last step of *selective coding*, we refined and integrated the results of the open coding and axial coding process to form a larger theory. Table 2 shows a small sample of our data analysis process.

The first author exhaustively coded all interview transcripts and conducted analysis to identify themes relevant to our research questions. The third author performed a second analysis for 20 percent of the transcripts (i.e., transcripts for three child-parent dyads) based on codes that emerged from the original analysis. A Cohen's Kappa ($k$) test showed that there was strong agreement between the two researchers' analysis, $k = 0.93$ (95% CI, 0.86 to 1.00), $p < 0.005$.

| P. # | Pseud. | Age | Gen. | P. # | Pseud. | Age | Gen. |
|---|---|---|---|---|---|---|---|
| **1.** | Ella | 8 | F | **8.** | Tyler | 10 | M |
| **2.** | Alex | 7 | M | **9.** | Luke | 11 | M |
| **3.** | Jake | 11 | M | **10.** | Adam | 9 | M |
| **4.** | Mary | 9 | F | **11.** | Anna | 8 | F |
| **5.** | Kyle | 7 | M | **12.** | Maya | 7 | F |
| **6.** | Ryan | 7 | M | **13.** | Lily | 8 | F |
| **7.** | Ava | 9 | F | **14.** | Dave | 8 | M |

**Table 1. Child participants organized by their participant number, pseudonym, age, and gender.**

To protect the participants' identities, we will refer to each child by a pseudonym, followed by their age and gender (e.g., Ella, 8f). The adult participants will be addressed directly as the child's parent (e.g., Ella's mother). Their pseudonyms and demographics are summarized in Table 1.

## RESULTS

To provide context for subsequent sections on Children's Privacy Models (Section 4.2), Children's Threat Models (Section 4.3), and Parental Threat Models and Protection (Section 4.4), we begin the results with our findings on children's general device use, account management, and password management to understand the roles that children and adults play in the usage of mobile devices within the home environment.

### Children's Interaction with Mobile Devices

#### *Children's screen-time activities*

Our results showed that children engaged in limited types of online activities and had very small online social circles. They used mobile devices primarily for entertainment and were consumers rather than creators of online content.

Playing games and watching YouTube trumped all other activities on mobile devices. All of the children regularly used the devices for gaming. Some popular games mentioned include Minecraft, Tettoria, Clash of Clans, and Dragon City. Most children (12/14) also watched YouTube videos. They were attracted to "funny" and "hilarious" content, Minecraft clips, game tutorials, and episodes from popular kids TV shows. None of the children posted online content or write comments. About half of the children watched Kids' Netflix (6/14) and used a search engine (7/14) primarily for school related work. Texting/messaging (4/14) and email (4/14) were less common and exclusive to family, teachers, or friends that the child know offline. Other less frequent activities reported were listening to music (2/14) and using the device's camera to take pictures (3/14). Only two children had social media – one had a Facebook account that is used for playing games, not for posting or commenting; the other had an Instagram account for sharing pictures with family members. In both cases, parents set up the accounts with the highest privacy settings, and only close family members could view or comment.

#### *Device sharing*

The most popular device used among children were tablets (10/14), followed by iPod Touch (3/14), and handheld gaming

| CATEGORY: Code Name | Code Description | Behaviour code | Behaviour Description |
|---|---|---|---|
| MEDIA: Inappropriate content | Parental control is set for YouTube, Parents monitor what apps children have on their devices daily. Mom deletes violent or frightening games immediately. | Parental control, Monitor | Parental control is set for YouTube. Mom monitors apps. Mom deletes games with violent or frightening scenes. |
| TECH: Device addiction | Kids go on the devices too often; parents try to limit the hours when they can. Parents "don't get" the value of certain activities like feeding a virtual character. | Limit screen time | Parents try to limit how many hours kids spend on their device. |
| MEDIA: Inappropriate apps | Kids accounts are linked through mom's email. Mom created email to get iTunes. | Account linking, Monitoring | Mom can see what the kids are downloading. It pops up in her email. |
| MEDIA: Social media | There's a lot of inappropriate content on social media. Privacy settings are set high even for adults. | Restrict access until older, Account access, Monitoring | Mom thinks kids are too young; Facebook is unnecessary for their age. If they get Facebook, mom would closely monitor the account and have her password. |
| STRANGERS: Stranger-Danger MEDIA: Over sharing SELF: Kids are innocent and naïve | Mom worries about kids over sharing information and talking to strangers whose true identity is unknown. | Restrict access until older. Monitoring, Educate about the threat | Mom restricts access to social media, and monitors what they download. She talks to them about stranger-danger. |

**Table 2. A portion of the threats and behaviours identified for one parent in the open coding process. The threats are organized by code names, then put into related categories based on the initial step of the axial coding process. Each threat is mapped to an associated parental behaviour.**

systems (1/14). Children preferred tablets due to the large screen size. All households owned secondary devices that the children occasionally used, including other tablets, iPods, iPhones and Android phones, but none owned a mobile phone for the children's personal use.

Common among all families in the study was that one or more devices in the household were shared at least occasionally between siblings or with the parents. Parents shared their smartphones with their children primarily for convenience since they restrict children from taking their own devices outside of the house for fear of loss or damage. Parents often lent their smartphones to children to keep them entertained. In households with more than one child, devices were often shared between siblings.

### *Account management*

In all families interviewed, parents were responsible for the management of children's online accounts. The types of accounts that children used were for downloading apps (e.g., App Store, Google Play Store), email, online gaming, and social media. Children's online accounts were always created and managed with an adult's help. Parents always had full access and knew the passwords for monitoring account activities and account recovery in case the child forgets the password.

For services requiring credit card information (e.g., App Store), children used their parent's account with permission. Half required explicit consent from the parents to download apps. Parents either entered the password directly on the device, or managed a linked account where app download requests were forwarded to the parents' phone. The other half was allowed to download free apps on their own, but must receive permission prior to download. Additionally, parents periodically screened the mobile device to weed out 'bad' apps and many used parental control tools. In both groups, parents made the ultimate download decision and had the final say in whether an app can be kept or deleted.

Many children (9/14) owned email accounts that they did not use. The parents explained that the emails were created on occasions when the child needed it to sign up for another account. Adam's mother said that her son *"wanted to play the Facebook game," and "he needed an email to get a Facebook account"*; Maya's mother created an email account so her daughter could get iTunes; Anna's mother created the account to sign her daughter up for a game. Parents also set up emails for future use. For convenience, Anna's mother set up email accounts for all of her kids when the eldest started school, even though the younger siblings did not yet need them. Ryan's father prepared an email account for his son as an upcoming 'birthday gift'.

### *Password management*

The burden of remembering passwords for children's accounts usually fell on adults (parents and teachers). In the largest family we interviewed, all five children had individual email accounts and passwords managed by the mother (Adam's mother). Children frequently forgot their passwords, and for this reason, they were encouraged by parents and teachers to create easy to remember dictionary passwords (e.g., 'apple'). Adults always had a copy of the account information. If the account was created for school, the teacher provided parents with the login information. Not surprisingly, many adults used coping strategies like writing passwords down. To highlight the challenges and risks, we give Mary's mother's story of an incident at school:

> The teacher had passwords written down because apparently, [the email accounts] are setup with the school board

> and if the kids were to loose their passwords, they have to try to call somebody at the school board, which could take some time, which means the kid wouldn't be able to get into the account. So, the teacher had written all the passwords down and hid it in her desk. I think one of the students saw, copied some, and then hacked in.

All of the children had a basic understanding that passwords are secrets, but very few could explain why passwords should not be shared. Some examples from our interviews are: Kyle (7m) thinks that passwords should not be shared simply because "no one wants you to know what it is!" His parents do not share their passwords with him, and therefore he should not share his passwords with others. Ava (9f) might share her password with a friend that she trusts. Tyler (10m) revealed his iPad unlock PIN to his friends "because they are not going remember it." Alex (7m) could not explain why sharing is risky but stated that he *"just [don't] feel like it sharing it."* One parent (Jake's father) suggested, *"It's intuitive not to share it,"* because *"they'll know my passwords are secret before they get their own passwords."*

Children had a very vague definition of who constituted a stranger. For example, Ryan (7m) believed that it is acceptable to share passwords with somebody he already knows like his best friend. Strangers approved by parents were considered safe, such as the researchers who interviewed them. One child (Maya, 7f) blurted out her password that her mother made for her during the interview. Contradictory to her behaviour, the child also said that she would not share her passwords with her mother (even though the parent made the password), brother, or strangers.

### Children's Privacy Models

#### *Four models of children's privacy*

Livingstone [9] suggests that definitions for the concept of privacy are either centred on keeping information out of the public domain or centred on determining (or controlling, or knowing) which personal information is available to whom. Half of the children interviewed showed a lack of understanding about what it means to be private online. From their explanations, we identified four privacy models. Children with the first two models resorted to traditional definitions of physical privacy like 'to be alone', or 'to hide secrets or special things'. Children with the remaining two models had a preliminary understanding of online privacy that is based on notions of safety like 'to keep things to yourself' and 'to not talk to strangers'.

To children, privacy means:

***To be alone:*** This group accounted for 36% (5/14). 'Privacy' is analogous to 'being alone' or 'to be by myself.' Several of the descriptions involved physically confining oneself to a room such as *"if you need to go somewhere and you want it to be private, you shut the door and you really lock it"* (Mary, 9f); *"When you are taking a shower, and no one's coming in. You are in the room by yourself"* (Tyler, 10m). One child described instances when he should leave other people alone because they are doing something 'bad' on the computer and they don't want [others] to look. In that case, *"[others] should just leave them alone"* (Dave, 8m).

***To hide secrets or special things:*** Three children believed that being private is *"when you hide something, . . . something that's very special"* (Maya, 7f). Maya referred to hiding a physical item like her iPad, because *"you could have a little brother and they could break something."* Other children referred to hiding a secret that *"you don't want anyone to know"* (Kyle, 7m), and that you should *"not tell people what you have like stuff that you are not supposed to tell other people, like passwords"* (Ella, 8f). However, this was the only secret thing that Ella could identify.

***To keep things to yourself:*** Four children had a basic understanding that online privacy is *"keeping your things and events in your life to yourself"* (Luke, 11m); things like *"your own personal data, which people can take and you want to keep them private for only yourself"* (Adam, 9m). Jake (11m) also believed that he should not give away anything about himself that is too personal. Ava (9f) cautioned that you should not *"post anything you don't want to post. If you post it, you might regret it later"*. All four children with this model are in the older age group (ages 9-11).

***To not talk to strangers:*** Two children believed that *"privacy means you don't go lurking around people that you don't know, like you don't go play a game with a teenager that wants to know who I am and where I live. It's about keeping it safe"* (Ryan, 7m). Anna (8f) believed that being private means you should avoid the risks of someone *"being rude to you"* online. Both descriptions of privacy were framed as safety concerns.

### Children's Threat Models

Children identified four types of child/adversary threat models that concerned them: child-peers, child-parent, child-stranger, and child-media. Children had little protection strategies of their own. Their response to a threat is usually evasive or reactionary, such as avoiding content with 'bad' words or becoming 'upset' when something bad happens.

#### *Threat: peers*

Most children (12/14) considered siblings, friends, and other kids to be a threat they face on a day-to-day basis. The children in our study lived in homes with at least one other sibling. Adam (9m) for example, shared his device with four other siblings. Children constantly fought over screen-time on shared devices. Dave (8m) explained, *"I don't like (my brother) there because he always touches the iPad when I'm trying to watch a video."* Siblings could also damage children's special things so they need to be protected. Maya (7f) complained that her little brother *"always tries to blow up [her] stuff"* on Minecraft. Other risks of sharing a secret with siblings were that they are *"bad at keeping secrets"* (Luke, 11m).

Children also protected themselves from their friends. For example, when asked about whether they shared passwords with friends, Tyler (10m) said 'no', because *"they could send something to somebody, like say a bad word, and [he] could get in trouble."* Ava (9f) would not trust her best friend with her password because "she's done things" before. For game accounts, children's main concern was that others could 'mess up' their game if they had access. Ryan (7m) explained, *"it might be a little dangerous [to share my password], because*

*they would be able to play as me and do things that you know, like mess up my game. They can sell cars or they'll just spend all my money in the game, and then I'll have completely no money and then I can't upgrade my powers or anything."*

*Threat: 'bad' media*

Nine children identified media as a potential threat but had a vague understanding of the harm. Swearing, violence, and adult content were described as 'bad'. Kyle (7m) said he would not watch violent stuff online, only 'funny stuff.' Mary (9f) was aware that she was not allowed to get any apps with guns or watch videos with violence. Dave (8m) did not think he had any 'bad' games because he was not allowed to download a gun game that he wanted. He watched YouTube videos from a 'safe' channel that did not contain swear words. Anna (8f) thought there are 'bad' words on Facebook. When inquired about why those things were 'bad,' most of the children could not explain. Alex (7m) knew that he was not allowed to watch violent videos, but was confused about why he was allowed to *"watch stuff with swords but not guns"*. Most of the children had a very abstract understanding of these concepts and appeared to be following the rules set by the adults out of respect.

*Threat: 'mean' strangers*

Most children believed that you should not talk to strangers offline. Ryan (7m) said, *"stranger-danger I learn almost everywhere I go."* However, we found that only 33% (5/14) of children viewed it as an online threat. Strangers are typically judged by their friendliness online. The perceived harm from strangers is often viewed as trivial, such as being teased. Anna (8f) thought that you might want to hide things from a stranger, such as your real name so people could not make fun of your funny middle name. Jake (11m) believed that it was acceptable to show other kids pictures of yourself but maybe not older people, because *"younger kids are not allowed to do certain things but older kids are."* One child (Alex, 7m) felt that giving personal information to strangers have no direct impact on himself, but might cause dangers to others. For example, he said that he would not tell a stranger where he goes to school because *"they might not be nice and they are going to rob the school."* Only two children (Ryan, 7m, and Kyle, 7m) we interviewed perceived it as a real threat:

> You don't know if he's actually friendly or just hanging friendly. Then when you meet him in real life, he wants to hurt you or something. You don't go lurking around people that you don't know, like you don't go playing a game with a teenager that wants to know who I am and where I live. It's about keeping it safe. (Ryan, 7m)

Kyle (7m) said that staying safe online means not contacting anybody who is 'not nice' because they might try to bully him. Most of the other children's perception of the harm caused by strangers suggests that they do not see stranger-danger as an imminent or serious threat online.

*Threat: parents*

Four children saw parents as a risk to their privacy and special things, but were generally obedient to whatever rules or punishment that the parents imposed on them. They respected their parents' wishes even though they did not always understand why. For example Tyler (10m) said, *"I'm usually not allowed chatting with people, like people playing a game, but I feel like you're allowed to talk to them... but I don't. My mom doesn't want me to do it."* Maya (7f) expressed annoyance that her parents delete her apps. Adam (9m) cleared his browsing history to evade monitoring. Several of the parents took away the children's device as punishment when they misbehaved and this was sometimes viewed as a threat.

### Parental Threat Models and Protection Strategies

Parents identified five types of child/adversary threat models: child-media, child-technology, child-stranger, child-peers and child-self. To protect children against the threats, we found that parents employed a set of protection strategies, summarized in Table 3.

*Threat: media*

Children's exposure to inappropriate online media is one of the top concerns. Most parents interviewed (13/14) expressed worries about the content/media that children could access on their mobile device. We identified three sub-categories of such threats. For each of the sub-categories, we first describe the threat from the parents' perspective, and then describe the protective measures practiced.

***Inappropriate content:*** The 'inappropriate content' described by parents pertains to sexual and violent content, cruelty, coarse language, and other types of adult content. All of the parents expressed explicit concerns about children accessing inappropriate content even though only two parents had actually experienced a real incident with their children. Alex (7m) was caught watching a YouTube video that contained guns and violence, and Ella (8f) was found watching a video that contained sexual content at a friend's house.

Parents *Restrict-Access* to videos that are not age appropriate, and they demand the children to *Unplug-as-Punishment* if they misbehaved. Dave's mother thought that children are generally aware of what parents consider 'bad,' but they sometimes get confused if it is an adult cartoon (e.g., South Park). Parents *Set-Parental-Control* for YouTube, Netflix, and browsers. They regularly *Check-Browsing-History* and *Monitor* what children search and download on their devices. If violent or frightening games were found, parents would *Delete-Apps* immediately. Many parents wanted to know more about the app before the child downloads it. Parents used a variety of ways to *Screen-Prior-to-Download*. They judged the appropriateness based on how the app looked, game description, reviews, and age rating, but the outcome was not always reliable. Kyle's parent described an incident when they thought an app contained a bad word:

> The small thumbnail picture [of the app] had the word 'flick' on it... but the 'l' and the 'i' are mixed together and I thought it was an 'U', and so then I said that it had a really bad F-word on it and that he wasn't allowed to play that game because I didn't want games with that word. So, one of his friends said, 'I have that game, there are no bad words,' and then he said something about you

| Protection Strategies | Description | M: Inappropriate Content | M: App Permissions | M: Social Media | T: Device Addiction | T: Falling Behind Tech. | ST: Strangers | P: Older Siblings | P: Friends | S: Self |
|---|---|---|---|---|---|---|---|---|---|---|
| *Monitor* | Parent oversees device interaction. | ♦ | | ♦ | | | ♦ | ♦ | ♦ | ♦ |
| *Access-to-the-Account* | Parent has full access to the account. | | | ♦ | | | | | ♦ | ♦ |
| *Link-the-Accounts* | Child's account is linked to the parent's account. | | | | | | | ♦ | ♦ | |
| *Ask-for-Permission* | Child asks for permission before use. | ♦ | | | | | | | | |
| *Prohibit-Use-Until-Older* | Access is prohibited until the child is older. | | | ♦ | | | ♦ | | | |
| *Restrict-Access* | The child does not have access. | ♦ | | | | ♦ | | | ♦ | ♦ |
| *Limit-Screen-Time* | The child's time on the device is limited by the parent. | | | | ♦ | | | | | ♦ |
| *Delete-Apps* | Parent removes apps from the device. | ♦ | ♦ | | | | | | | |
| *Screen-Prior-to-Download* | Parent approves or denies app downloads. | ♦ | | | | | | | | |
| *Screen-Contacts* | Parent approves or denies whom the child can contact. | | | ♦ | | | ♦ | | ♦ | |
| *Check-Browsing-History* | Parent checks child's browsing history. | ♦ | | | | | | | | |
| *Set-Parental-Control* | Parent uses parental control tools. | ♦ | | | | | | ♦ | | |
| *Check-Privacy-Settings* | Parent sets privacy settings. | | | ♦ | | | ♦ | | | |
| *Check-App-Permissions* | Parent checks what apps have access to on the device. | | ♦ | | | | | | | |
| *Educate-About-the-Threats* | Parent speaks to the child about the threat. | | | | ♦ | | ♦ | | | |
| *Unplug-as-Punishment* | Parent denies access to the device if the child misbehaves. | ♦ | | | | | | | | |
| *Update-Tech-Knowledge* | Parent keeps technology knowledge up-to-date. | | ♦ | | | ♦ | | | | |
| *Use-Safe-Texting* | Child can only send predefined messages. | | | | | | ♦ | | | |

**Table 3. Summary of protection strategies used by parents to protect children against each perceived threat.**
**M = Media, T = Technology, ST = Strangers, P = Peers, S = Self, ♦ = Parent uses the protection strategy.**

> have to 'flick' things away, and I said 'oh, it says flick. Oh!' And then we understood.

A few other parents read app recommendations from parenting magazines. Mary's parent admited that sometimes choosing apps is a matter of 'trial and error,' but parents could always *Delete-Apps* later.

All of the children *Ask-for-Permission* to download an app, even though half could download free apps on their own. Half of the parents *Restrict-Access* to password protected accounts for purchases, such as the App Store or iTunes.

***App permissions:*** A few parents worried about the things apps could access on the mobile device, such as the camera, photos, microphone, location, and personal and financial information. Tyler's parent shared a story she learned on the Internet with her son about the app 'My Talking Angela' (a chatterbot app) to teach him about the danger. The app was rumoured to encourage children to disclose personal information using the game's text-chat feature, which was then exploited by pedophiles. The incident was a hoax spread on the Internet, but it highlighted fears from parents about what apps could access on their children's devices.

Surprisingly, very few parents from this group actually read app permissions during downloads. We found that parents used a 'trial and error' method to periodically *Check-App-Permissions* in game settings after the apps were downloaded, and *Delete-Apps* if they felt they accessed too much information. For example, Mary's parent described her reaction to a game called Clumsy Ninja that had hidden features:

> Sometimes it's a trial and error where [my daughter] gets something and then all of a sudden I will see, like there's a ninja one that she has, that you can take pictures on. I saw it, deleted it, read about it, she got it again... the pictures go to our pictures file. So sometimes, it's trial and error where I didn't realize that it had any picture or video options.

Some parents reported difficulties in managing app settings. *"It's pretty complicated"*, said Adam's parent, *"it seems like every company is making it more complicated for people to access their privacy settings, and it's frustrating."*

***Social Media:*** Our findings from Section 4.1 suggest that children aged seven to eleven have minimal interactions with social media. Only two children used a social media account and they did very little with it. Parents *Check-Privacy-Settings* and *Screen-Contacts* to ensure that only family and close friends can contact the child. Only 4 parents (29%) were worried about social media since most children did not have access. Parents explained that children *"are too young"* and that *"[social media] is unnecessary"* for their age (Maya's parent). The parent elaborated further, *"I mean, what are they going to do on there? There's a lot of things that come up on there that is inappropriate. You know what I mean? Even for myself my privacy settings are so high. So yeah I think she's too young. I don't see her using that for quite a while."* Most of the parents believed that the appropriate age for social

media is around 11 or 12 years old. *"We haven't said 'no' to Facebook,"* Anna's parent clarified, *"but right now the answer is no. She has asked a couple of times, but no you are eight! I know what comes across my feed! I think a lot of people put too much of their business on there I think that's dangerous."*

Parents expressed their resolve to Prohibit-Use-Until-Older, and for *"as long as they can"* (Anna's parent). All parents from this group said that if their children were to get social media, they would demand *Access-to-the-Account* and closely *Monitor* its use.

#### *Threat: technology*

Six parents (43%) worried about the impact of technology on children. We identified two sub-categories this threat. The first category describes parents' effort to limit the use of technology for the fear of device addiction. The second category describes parents' anxieties to keep up with technology to properly protect their children.

***Device addiction:*** Most parents limited the duration of device use from 20 minutes to one hour on weekdays and longer on weekends. Many parents voiced concerns about children spending too much time on their mobile devices. If parents did not *Limit-Screen-Time*, kids will *"go on it all day if they can"* (Maya's parent). Parents *Educate-About-the-Threats*. Mary's parent elaborated: *"We had a talk about addiction. We explained that addiction could be to the technology, to games... If I would allow it, she would be on her iPad for like 8 hours straight. She would even skip meals. She's very stimulated by the colours, movements, music, and sound on the iPad." "She's very smart,"* the parent continued, *"she can see that we are pre-occupied with her sister or supper, and she would say, 'I have to go to the washroom,' and she'll go and try to sneak in a video..."*

Despite the effort, parents found it *"hard to get away from screen time, because there's so much movies that are online that you want to watch. There's so much learning material for children, but it's so convenient that it became an inconvenience"* (Adam's parent). Parents wanted more human-to-human interaction with their children. One parent also expressed frustration that she did not understand the value of certain game activities like feeding a virtual pet on time (Maya's parent).

***Falling behind technology:*** Parents who were not technologically savvy expressed fear of falling behind the technology used by children. Dave's mother felt that keeping up with technology and knowing what kids are into is the only way to properly monitor them. Ava's mother was also troubled by the fact that kids *"know a lot more [than her]"*, and described how she spent three hours with a consultant when she purchased a mobile device for her daughter to learn about the settings, parental controls, and other functionalities of the device. *"This is what my daughter is going to be doing with it,"* she said, *"I want to be able to monitor it."* Parents either *Update-Tech-Knowledge* or *Restrict-Access* to unfamiliar technology. Ava's mother admitted, *"I limit technology because I'm not very savvy with it and I don't want her to be getting into things that are too far over my head that I can't monitor."*

#### *Threat: strangers*

Threats from strangers, dubbed 'stranger-danger' by the parents, were identified by the majority (13/14) as a major concern, even though none of the children had an incident with a stranger online. Parents worried about children over-sharing information about themselves and talking to strangers whose true identity is unknown. Maya's mother commented,

> *There are certain people on YouTube who play (Minecraft) and [my daughter] wants to meet them and I'm like no, that's not going to happen. I've talked to her about privacy, about what's appropriate and what's not appropriate, what you should or should not be giving out.*

Most parents agreed that children have the basic knowledge to not talk to strangers offline because they learned about 'stranger-danger' and 'bullying' concepts from a very young age. For example, Ryan (7m) learned about these concepts from a karate teacher. However, there's a disconnect for them between online and offline dangers. *"I worry about that,"* said Anna's mother, *"especially my son. He's the friendliest kid you'll ever meet. He loves to talk and he loves to be everybody's friend, so that worries me. He knows in person not to talk to strangers, but of course online is totally different."* Adam's parent also believed that kids have the basic knowledge about safety like not giving out phone numbers, but are naïve about other things. Maya's mother worried that kids would *"not know things like you think you are talking to Donna and it's really Joe that's 45."* Similarly, Kyle's parent said that the thought of enabling children to contact other people made her nervous. Alex's mother also did not allow her son to chat online because *"you never know who's on the other side."*

Most children had online access only to people with whom they also had offline contact. Parents *Screen-Contacts* so that children could only send text messages to family and close friends. For example, Kyle's parent said,

> He's got very few addresses in there. So it's only the people that we know and approve of that he can text, like his uncle or his stepbrothers. Sometimes he'll take funny pictures of toys that they are playing with and send those. Or sometimes if he is with his dad and he's built something cool out of Lego or something, he'll take a picture and text that to me.

Parents generally *Prohibit-Use-Until-Older* of online chat and text messaging apps. They *Monitor* who they talk to, and *Educate-About-the-Threats* such as talking to strangers online. They gave advice such as *"avoid answering questions unless you know exactly who the person is, like your friend across the street"* (Jake's parent). For the few children with social media, parents *Screen-Contacts* and *Check-Privacy-Settings* to ensure that they cannot be contacted by strangers. Some parents *Use-Safe-Texting* apps so that the child could select from a set of predefined messages. For example, Tyler (10m) could send generic messages like 'good luck' to communicate with other players in an online game. Mary (9f) used a safe-texting app connected to a doll where she could send text messages and chat with the doll.

*Threat: peers*

Some parents (8/14) believed that online dangers could be caused by another child, usually the child's friends and older siblings.

***Older siblings:*** Older siblings could expose inappropriate content to younger siblings. Parents found it difficult to *Set-Parental-Control* when there are multiple children living in the household. Ella's mother explained,

> What [my older daughter] is aware of and knows is very different from what Ella is aware of and knows. [my older daughter] already had sex education and she's in grade 5. She's aware of that and Ella isn't. As a parent, I would like to maintain that innocence, so the games should just be fun, interactive, and age appropriate. Some of the older games are very age inappropriate, you know, big boobs... that's for teenagers.

Parents did not have good strategies for protecting children from older siblings other than to *Monitor* them. Some parents *Link-the-Accounts* between siblings for easier monitoring.

***Friends:*** Parents felt that children's friends have a huge influence. Most parents said they trusted their own children, but were wary of their friends. Ava's mother explained, *"she's very responsible. Sometimes the kids themselves are not mischievous but it's their friends that are instigators. They don't understand the influence that others have on them."* Ella's mother described an incident when her daughter slept at a friend's house and they decided to check out a porn site. Parents worried about losing control of what the child is exposed to outside of their own homes. Adam's mother said, when they *"go to their friend's house, I can't control what they get from their friends."* Lily's parent worried about social influence, peer pressure, and the type of friends they talk to.

Parents have *Access-to-the-Account* and regularly *Monitor* account activities. Tyler's mother goes through the child's text messages secretly at night when he is asleep. Parents *Screen-Contacts* on mobile devices and on social media. Some parents *Link-the-Accounts* to their own device so they can *Monitor* activities. When a certain friend is over for a visit, Ava's parent *Restrict-Access* to devices to reduce chances of getting into mischief. Parents *Screen-Prior-to-Download* any games recommended by a friend.

*Threat: self*

Half of the parents believed that children are young and naïve and therefore should be protected from potential harm caused by their own actions. A common attitude among the parents was that *"kids will be kids. They are curious and want to try things"* (Ella's mother). Children are sheltered by parents from any potential external harm. Jake's father explained:

> Right now they are kind of at the innocent stage of using iPads or technology where they have been shown how to do something... how to specifically do a few things and not much about... I don't even think he has really gone on the Internet on the iPad before, it's really through applications and that's it. My daughter is the same way. They are very limited in their understanding and knowledge of what these things can do.

Children were either deliberately not exposed certain technology, or they were restricted from accessing certain tools or services. Ryan (7m) explained that his father would not give him his App Store password *"because he thinks I'd buy any random game. All the games!"*, but Ryan explains that he would not do that because he is selective of the games he likes. He also said that he was curious about sharing some pictures that he took on mom's Facebook page, but was told that he is not old enough for the activity. Children were therefore limited in their usage of some technology and from partaking in certain social activities.

Parents *Monitor* children to protect them against self-inflicted harm. If the child has an online account, they usually have full *Access-to-the-account*. They would *Prohibit-Use-Until-Older* of certain tools and services. To prevent children from spending too much time on mobile devices, parents *Limit-Screen-Time*.

## SUMMARY OF KEY FINDINGS

We summarize the findings based on the three research questions we set out to answer.

*R1) Children's privacy:* Children's understanding of external threats is very basic and reflects their experiences with offline safety. Therefore, the majority of the children's privacy models consist of 'to be alone' or 'to hide secrets or special things'. Others showed rudimentary understanding that privacy means 'to keep things to yourself,' or 'to not talk to strangers.'

*R2) Perceptions of potential threats:* We identified four threat models perceived by children aged 7 to 11 and five threat models perceived by their parents, summarized in Table 4. Our results show large discrepancies of perceived threats within the child-parent dyads. Most children (11/14) thought friends and siblings posed a threat because they could tamper with their device, compete for screen-time, 'mess up' their game, or do things on the device that could get them into trouble with adults. Dangers coming from media (9/11) were mainly exposure to bad words, violence, and other adult content, but the real harm perceived by children seemed to be the punishment from adults for viewing 'bad' content. Threats from strangers were brought up by a small number of children (5/14), but the risks perceived were limited to getting teased or bullied. Parents on the other hand, perceived more severe external risks from peers (9/14), media (13/14), and strangers (12/14). Additionally, they identified threats from technology (6/14), and from the children themselves (7/14).

*R3) Strategies to protect children:* Parents protect children against potential threats by exercising a variety of protection strategies (See Table 3). Our findings from *R2* suggest that a relationship exists between the perceived threats and the protection strategies used; most protection strategies are intended to protect children from external threats.

Children and parents' perceptions of threat models help to explain how they prevent internal and external threats. Parents employed protection strategies to protect children mainly

| Child's Threat Models | Ella | Alex | Jake | Mary | Kyle | Ryan | Ava | Tyler | Luke | Adam | Anna | Maya | Lily | Dave | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Child-peers | ★ | ★ | | | | ★ | ★ | ★ | ★ | ★ | ★ | ★ | ★ | ★ | 11 |
| Child-media | | ★ | ★ | ★ | ★ | ★ | ★ | | ★ | | ★ | | | ★ | 9 |
| Child-stranger | | ★ | ★ | | ★ | ★ | | | | | | ★ | | | 5 |
| Child-parents | | | | ★ | | | | ★ | | ★ | | ★ | | | 4 |
| Parent's Threat Models | | | | | | | | | | | | | | | |
| Child-peers | ♦ | | | | ♦ | | ♦ | ♦ | | ♦ | ♦ | ♦ | ♦ | ♦ | 9 |
| Child-media | ♦ | ♦ | | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | 13 |
| Child-stranger | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | | ♦ | ♦ | ♦ | ♦ | | 12 |
| Child-technology | | | | ♦ | | | ♦ | | | ♦ | ♦ | ♦ | ♦ | | 6 |
| Child-self | ♦ | | ♦ | | | ♦ | | | | ♦ | ♦ | ♦ | | ♦ | 7 |

**Table 4. Comparative summary of the threat models we identified in parent-child dyads.★ = Child has the model. ♦ = Parent has the model.**

from perceived external threats that may or may not pose real dangers to children; they were often exercised at the cost of invading children's privacy. Children's threat models were conceived based on their perception of physical privacy. There were major differences between children's and adult's threat models that could influence their privacy-preserving behaviour.

## DISCUSSION

Consistent with literature on children's use of mobile devices [10, 13, 19], we found that their primary activities are playing games and watching videos. Younger children do not manage their own accounts or passwords. They have small online social circles, which consisted of family, extended family, and close friends only.

As it might be expected, there is a clear gap between threats perceived by children and adults. Children showed less concern for online dangers because they do not yet know how to apply the concept of privacy online. The protection strategies practiced by the parents suggest that the lack of apprehension is largely due to the fact that young children are strongly sheltered by parents from having an online presence. Our findings show that parents perceived external threats (i.e., media, strangers, peers-friends, technology) to be more prevalent than internal threats (i.e., self, peers-siblings). In reality, we found that security and privacy risks from an internal family member or a friend are far more common than harm caused by cybercriminals or outsiders. For example, even though the majority of parents (13/14) believed strangers to pose a serious threat to children, none had experienced an incident where a stranger contacted a child online. It is difficult to determine however, whether parents' protective measures directly resulted in the reduction of external risks encountered by their children. Even so, our findings suggest that it is much more likely that children experience invasions of privacy and security from other members of the household, from friends, and from teachers. Children are constantly put under adult surveillance and do not have rights to privacy on their own accounts. Causes for breaches of security and privacy often came from a trusted adult. Several incidences came up in our interviews, including one described in Section 4.1.4 where a teacher wrote down all of the children's passwords and they got stolen by a student. Children were encouraged by adults to choose weak, easy-to-remember passwords, which could be quickly cracked in a dictionary password guessing attack. Most children owned unused password-protected accounts that were created by an adult. Although few children had an online presence on social media, parents frequently posted pictures of children on Facebook. Conversely, parents also faced risks from children. All parents interviewed shared at least one online account with their children, usually for making app purchases. Half of the children had access to the account (although they said they would still ask for permission first). They either knew the password, or had the password autosaved. Children could potentially misuse the account and credit card information. If they misbehaved under the account name, it could have a negative impact on the adult's credibility. Some security threats from children identified by the parents were password guessing, shoulder surfing, unauthorized access to device or apps, disclosure of parents' information to others, and losing the device with the account information.

Parents were conflicted between wanting to teach kids about online dangers for safety, but they also wanted to shelter them from online negativity. Luke's mother explained, *"I wouldn't want to teach them about all the negative things that can happen... and I try not to go into detail about everything that's out there... they'll never sleep again."* Parents cautioned that children should not be exposed to privacy/security education too young. Parents feel that a lot of educational material is more suitable for older kids. Mary's mother described a presentation about online privacy at her child's school: *"The material is over their heads, like talking about Twitter and Facebook, which [the kids] are not really aware of."* Younger children need something that is relevant for their own age. We suggest that education about online privacy and security for young children should work with their existing privacy models to gently introduce them to the concepts. The four privacy models and four threat models from this paper could serve as a starting point.

### Limitations

In our study, we cannot estimate how prevalent the models we identified are in children and adults due to our small sample size. Our data also may not be exhaustive to cover all of the models existing in the population. We do however, contribute to the understanding of young children's interactions with

mobile media by putting forth a variety of children's privacy models and identified existing differences in the threat models perceived by children and their parents.

## CONCLUSION

This work suggests that children have different privacy and security needs than adults. Young children have underdeveloped models of privacy, and their threat models mainly consist of internal threats from family members. Ironically, our results suggest that the threats perceived by children are actually closer to the reality of privacy and security risks faced by families on a day-to-day basis. Risk from online predators, pedophiles, cyberbullies, cybercriminals, and other online dangers are less likely to occur for younger children due to their small online presence. Parents felt the need to safeguard children by limiting what they could access and who they could talk to online. They exercised a plethora of protection strategies that undermined children's privacy and at times unintentionally jeopardized the children's or their own security. This work highlighted some of the unique challenges faced by parents and children in managing their privacy and security.

## SELECTION AND PARTICIPATION OF CHILDREN

In our ethics approved study, children were recruited through public invitations shared with parents on local Facebook community groups and through email invitations sent to personal acquaintances. The participants lived in the regions of Ottawa, Kitchener-Waterloo, and Cambridge in the province of Ontario, Canada. Participation in the study was limited to children aged seven to eleven and to one child per family. Parents signed an informed consent form for their participation and a parental informed consent form to give permission for their child's participation. The forms included consent to be audio-recorded for the purposes of transcription. Additionally, the children provided verbal informed assent.

## ACKNOWLEDGMENTS

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the authors and do not necessarily reflect those of the OPC. S. Chiasson acknowledges funding from NSERC for her Canada Research Chair in Human Oriented Computer Security.

## REFERENCES

1. Tawfiq Ammari, Priya Kumar, Cliff Lampe, and Sarita Schoenebeck. 2015. Managing children's online identities: How parents decide what to disclose about their children online. In *Proceedings of ACM Conference on Human Factors in Computing Systems*. ACM, 1895–1904.
2. Farzaneh Asgharpour, Debin Liu, and L Jean Camp. 2007. Mental models of security risks. *Financial Cryptography and Data Security* (2007), 367–377.
3. Federal Trade Commission (FTC). 1998. Children's Online Privacy Protection Act. `http://www.coppa.org`. (1998).
4. Rebecca E Grinter, W Keith Edwards, Mark W Newman, and Nicolas Ducheneaut. 2005. The work to make a home network work. In *ECSCW 2005*. Springer, 469–488.
5. Uwe Hasebrink, Sonia Livingstone, and Leslie Haddon. 2008. Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online. *status: published* (2008).
6. Camp Jean. 2009. Mental Models of Privacy and Security. *IEEE Tech. and Society* 28, 3 (2009).
7. Sherri Jean Katz, Theodore Lee, and Sahara Byrne. 2015. Predicting Parent-Child Differences in Perceptions of How Children Use the Internet for Help With Homework, Identity Development, and Health Information. *Journal of Broadcasting & Electronic Media* 59, 4 (2015), 574–602.
8. Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2010. *Research methods in human-computer interaction*. John Wiley & Sons.
9. Sonia Livingstone. 2011. Children's privacy online: Experimenting with boundaries within and beyond the family. *Computers, Phones, and the Internet: Domesticating Information Technology* (2011), 128–144.
10. Sonia Livingstone and Magdalena Bober. 2004. UK children go online: Surveying the experiences of young people and their parents. (2004).
11. Gary Marx and Valerie Steeves. 2010. From the beginning: Children as subjects and agents of surveillance. *Surveillance & Society* 7, 3/4 (2010), 192–230.
12. Corinne May-Chahal, Claire Mason, Awais Rashid, James Walkerdine, Paul Rayson, and Phil Greenwood. 2014. Safeguarding cyborg childhoods: Incorporating the on/offline behaviour of children into everyday social work practices. *British Journal of Social Work* 44, 3 (2014), 596–614.
13. Common Sense Media and Victoria Rideout. 2013. Zero to eight: Children's media use in America: A Common Sense Media research study. `https://www.commonsensemedia.org/research/`. (2013).
14. Miriam Metzger, Andrew Flanagin, and Elmie Nekmat. 2015. Comparative Optimism in Online Credibility Evaluation Among Parents and Children. *Journal of Broadcasting & Electronic Media* 59, 3 (2015), 509–529.
15. Jenny Preece, Helen Sharp, and Yvonne Rogers. 2015. *Interaction design: Beyond human-computer interaction*. John Wiley & Sons.
16. Yvonne Rogers. 2004. New theoretical approaches for HCI. *Annual review of information science and technology* 38, 1 (2004), 87–143.
17. Stuart Schechter. 2013. The user is the enemy, and (s)he keeps reaching for that bright shiny power button. In *Workshop on Home Usable Privacy and Security (HUPS)*.
18. Benjamin Shmueli and Ayelet Blecher-Prigat. 2011. Privacy for children. *Columbia Human Rights Law Review* 42 (2011), 759–795.

19. Valerie Steeves. 2014. Young Canadians in a wired world, phase III: Life online. http://mediasmarts.ca/sites/mediasmarts/files/pdfs/publication-report/full/YCWWIII_Life_Online_FullReport.pdf. (2014).

20. Anselm Strauss and Juliet Corbin. 1994. Grounded theory methodology. *Handbook of qualitative research* (1994), 273–285.

21. David Swallow, Mark Blythe, and Peter Wright. 2005. Grounding experience: Relating theory and method to evaluate the user experience of smartphones. In *Proceedings of the conference on European Association of Cognitive Ergonomics*. University of Athens, 91–98.

22. Rick Wash. 2010. Folk models of home computer security. In *Symposium on Usable Privacy and Security (SOUPS)*. ACM.

23. Rick Wash and Emilee Rader. 2015. Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. In *Symposium on Usable Privacy and Security (SOUPS)*. 309–325.

24. Morris Williams, Owain Jones, Constance Fleuriot, and Lucy Wood. 2005. Children and emerging wireless technologies: Investigating the potential for spatial practice. In *SIGCHI Conference on Human Factors in Computing Systems*. ACM, 819–828.