usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

Youth understandings of online privacy and security: A dyadic study of children and their parents

Olivia Williams, *University of Maryland;* Yee-Yin Choong
and Kerrianne Buchanan, *National Institute of Standards and Technology*

https://www.usenix.org/conference/soups2023/presentation/williams

This paper is included in the Proceedings of the
Nineteenth Symposium on Usable Privacy and Security.

August 7–8, 2023 • Anaheim, CA, USA

978-1-939133-36-6

Youth understandings of online privacy and security: A dyadic study of children and their parents

Olivia Williams, *University of Maryland*[1], *College Park, MD, USA*
Yee-Yin Choong, *National Institute of Standards and Technology, Gaithersburg, MD, USA*
Kerrianne Buchanan, *National Institute of Standards and Technology, Gaithersburg, MD, USA*

Abstract

With youth increasingly accessing and using the internet, it is important to understand what they know about online privacy and security (OPS), and from where they gain this knowledge in order to best support their learning and online practices. Currently, the field of literature surrounding such youth understandings has gaps in depth and breadth that we aimed to address in this study. We conducted semi-structured interviews with 40 youth/parent dyads with youth in 3rd-12th grades in the United States to understand more about what youth know about OPS and how their parents attempt to influence this knowledge. We found that youth of all ages in the study could provide at least basic descriptions of both online privacy and online security and could give relevant examples of good and bad OPS choices. We also found that parents took a variety of approaches to influencing youth understandings and behavior, with most of those approaches relying on device monitoring and limiting use. However, parents who attempted to influence their children's knowledge through conversations had children who demonstrated the most nuanced understandings. Our findings offer promising suggestions for parents, technology providers, and future research.

1. Introduction

Children and teenagers under 18 (hereafter referred as "youth") utilize technology more and at younger ages than ever before [1], and are often "digital by default" [52] with digital footprints that begin before birth [53]. In 2019, 95% of 3–18-year-olds in the United States had home internet access [56]. With this access, youth of all ages participate in a variety of activities online—including gaming, researching, social media, emailing, and streaming entertainment ([1][28])—all of which involve elements of online privacy, security, and personal data management. As a result of this ongoing use, youth's descriptions and understandings of online privacy and security (OPS)[2] are constantly in flux as they learn how to protect themselves and be responsible in an ever-evolving online context ([22][60]).

To know how to best support youth's ever-developing OPS knowledge, we need to know more about the influences and intricacies of their current understandings, as well as the people and places—including parents, family members, schools, friends, and technology itself—that influence those understandings.

Quayyum and colleagues [44] reviewed a decade of youth cybersecurity awareness literature from 2011-2020 and concluded that "although cybersecurity awareness research for children has received significant attention from researchers, there remain gaps," particularly in evaluating youth's awareness [44]. The purpose of our study was to address this gap in order to learn more about what youth know about OPS. In addition, we wanted to understand how parents understand and attempt to influence youth's OPS knowledge and practices given the important role they play in youth's lives and access to technology. To achieve these purposes, we interviewed 40 youth/parent dyads with youth in 3rd-12th grades to answer three research questions:

1. What are youth's descriptions of online privacy and online security, and how do they understand these terms?
2. How do parents view the role of online privacy and online security in their children's lives?
3. How, if at all, do parents influence children's online privacy and online security understandings?

Our qualitative investigation of these questions is unique in two ways. First, the design of our study was distinct from its peer research in both its dyadic structure and in the broad age range of youth participants (3rd-12th grade). This design and population allowed us to compare youth and parent

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6 -- 8, 2023, Anaheim, CA, USA.

[1] This material is based on work supported by the UMD and NIST Professional Research Experience Program (PREP) under Award Number 70NANB18H165.

[2] We use OPS as an acronym for brevity when we are talking broadly about the focus of the study *or* discussing parental involvement in aspects of youth online activity that influence both online privacy and security.

understandings surrounding OPS across and within dyads and grade bands to look for interrelationships that cannot be studied using other research designs. Second, much of the extant literature surrounding online security knowledge, specifically, examines youth's knowledge after participating in some kind of learning experience like a cybersecurity game or summer camp (e.g., [24][50]). These studies are valuable in that they evaluate contexts and supports that help youth learn about OPS, but they also precludes the ability to know what and how children understand OPS in their day to day lives either before or without such targeted learning experiences. Our study, by contrast, explores youth's knowledge without any kind of OPS knowledge intervention in order to better examine what youth authentically know about OPS.

For the purposes of this study, we acknowledge that both "online privacy" and "online security" are broad, complex terms for which descriptions depend on audience and context. There is no commonly and widely used description of either term, which has been recently acknowledged by the field (e.g., [20][22][42]). Accordingly, in this paper we explore extant research involving youth knowledge of each term separately ("online privacy" and "online security"), and report out findings regarding our study participants' understandings of each term separately. However, we purposefully did not provide our own definitions of these terms given the study's overarching purpose of understanding how our participants describe and understand the terms through their own words and examples.

2. Related Work

2.1. Youth OPS Understandings

2.1.1 How Youth Understand Online Privacy

Youth's "needs, opinions, experiences, and attitudes towards privacy and data protection are the least researched so far"[37], due largely to the fact that many adults believe youth, especially young children, are too young to understand or care about online privacy [29]. That belief, however, is inaccurate. The research reviewed for this study agrees that youth as young as six have some knowledge and care about the basic idea of online privacy ([37][67]). These studies also reveal that although youth find online privacy important and have basic ideas about why it matters, these understandings are not nuanced.

Younger youth especially (up to age 11) have been found to value their privacy without fully understanding what it means to be private online [65], and to have flawed reasoning behind their understandings [5]. Youth in this age group have also been found to dislike the idea of their personal information being shared with strangers online, but do not always know how to prevent this from happening [44]. These gaps in youth's understandings are partially attributable to developmental processes: the concept of "online privacy" contains both tangible and abstract aspects that are complex, varied, and constantly changing ([8][18]). This can make it difficult for people of any age to learn about and exercise good online privacy behaviors, but especially youth, who do not begin processing abstract concepts until around age 12 [45]. Even as youth move into their teenage years, navigating abstract concepts like "privacy" and "security" takes time, and can be difficult to translate into online practice [45].

Further, online privacy can be broadly categorized into three "levels"—the interpersonal, the institutional (i.e., government organizations), and the commercial—that are all unique and need to be understood differently [32]. Because youth's developing online privacy understandings are an extension of their knowledge of privacy in the off-line world, they often have a strong sense of interpersonal online privacy (i.e., avoiding "stranger danger"), but have much less institutional or commercial privacy knowledge [52]. This is problematic, because the moment youth exist and interact online, their information and data are being collected. However, youth often have no idea what that means or what (if anything) they should do about it ([33][50]). This results in youth who are "cautious about strangers…[but] have not yet received knowledge about how corporate forces can use their data" [8]. This sentiment was echoed across multiple studies (e.g., [12][50]), with Milkaite and colleagues noting "when it came to their participants' [83 9-12-year-old] knowledge of data protection rights and of more detailed data processing actions, the purposes of data collection, sharing and general use in commercial and institutional contexts, children's understanding was much more limited" [37].

Finally, some studies show that youth—and especially older youth—view elements of online privacy as negotiable and choice-based, which contributes to something called the "privacy paradox" [23]. The "privacy paradox" is the notion that privacy knowledge does not always translate into privacy-protective strategies. For example, in a study of 366 4th-6th graders, this discrepancy between what youth know about privacy and if or how they put that knowledge into practice was common, and was most striking in the oldest (6th grade) youth in the study [15]. Similarly, a survey of 805 9-17-year-olds in Taiwan revealed that "performing privacy protective practices did not simply lead to fewer privacy-precarious practices" [10], suggesting that youth who had knowledge of online privacy took preventative measures while also maintaining questionable practices, or intentionally did not practice making choices that align with their knowledge of online privacy ([7][44]). It is important to note that the privacy paradox has been critiqued for its inability to sufficiently address the pervasiveness of technology in everyday life [60], and these critiques are in line with other calls to better address how the field needs to work on redefining ideas like "privacy" to capture new contexts like digital platforms [3]. Many such critiques include the online technologies and platforms most used by youth, making the critiques particularly important topics to consider in the youth user context.

2.1.2 How Youth Understand Online Security

A majority of studies exploring youth understandings surrounding online security focus on the impact of online cybersecurity games or interventions on youth knowledge (e.g., [11][41]). The result is that these studies do little to help explain what youth actually know without receiving targeted training first, or what they take away from learning about online security outside the minutes immediately following some sort of targeted instruction. It is likely that some of the same challenges with abstractness and developmental thinking that can make online privacy challenging to learn also apply to the process of learning about online security, but the topic is less well studied and understood.

In one of the few investigations seeking to broadly understand youth's cybersecurity awareness, only 19% of the 2,214 8-12-year-olds and 32% of the 13-17-year-olds surveyed in New Zealand recognized seven common cybersecurity terms [57]. Of those who did recognize terms, most of the awareness surrounded more fundamental ideas like firewalls and antivirus software with very few youth—only one of the 444 youth in the 8-12-year-old group—having an awareness of terms like "phishing" and "tracker" [57]. Other cybersecurity awareness surveys were conducted in Malaysia [68] and Turkey [63] with similar results: youth were found to have very basic levels of cybersecurity knowledge and awareness, and rarely took measures to increase their cybersecurity.

Most of the other available literature addressing youth's preexisting online security knowledge uses passwords as a vehicle to gauge this understanding, and this password-related literature is also reflective of the knowledge vs. practice paradox. For example, Theofanos and colleagues [56] found that in 8-18-year-olds, older youth had more password knowledge, but were also more likely to report using poor password practices like sharing passwords with friends or reusing passwords across multiple sites [56].

2.2. Framing Youth Knowledge and Behavior Through a Social Learning Lens

In this study, we use social learning theory [4] to frame our understanding of youth OPS knowledge and parents' potential influence on that knowledge. Social learning theory suggests that most human behavior is learned observationally through modeling and from one's surroundings; people learn from seeing or being taught something, trying it on their own, and then evaluating the results [4]. Through this lens, to better understand youth's OPS knowledge and behavior, we must better understand their contextual influences—such as parents, family members, friends, teachers, and technology itself—as well as what motivates youth to retain and actually use OPS best practices. In this study, we chose to specifically examine the contextual influence of parents because of how prevalent and influential parent relationships are in children's lives. A social learning framework led us to focus our data collection and analysis on how youth described and explained OPS and how parents described their roles in their children's OPS knowledge development to examine possible connections between the two.

2.3. Parental Influence

In terms of contextual influences on youth's OPS knowledge, parents are a natural point of inquiry given their central role in youth's lives. Especially up until around age 11, youth rely on their parents for support with OPS choices and tend to seek out and accept parental oversight and support [33]. What extant literature otherwise knows about parents' influence on youth OPS understandings, however, is complicated. For example, Manotipya and Ghazinour surveyed 1,300 parents from 51 countries and found that parents generally feel that they have some awareness of their children's online privacy practices, but that parents also often pose a threat to their children's privacy by oversharing information online ([19][34]).

Device monitoring tends to be a common practice for parents to influence their children's OPS. In an interview study about child internet use and protection strategies with 14 families, 18 protection strategies were found, 17 of which were physical or technical controls like restricting access, configuring privacy settings, and restricting access as punishment [64]. Despite its widespread use, device monitoring may only be effective with younger youth. In a study of 1,700 4th-6th grade students' internet use and supervision, about half of the students reported being supervised when using the internet at home. Those youth who reported some level of parental oversight were more likely to practice privacy protective behaviors [59]. A separate survey of 746 12-18-year-old youth, however, told a different story. Unlike their 4th-6th grade counterparts, the teenagers surveyed by Shin and Kang [48] who experienced device monitoring and use rules did not demonstrate more privacy-protective behaviors. This reflects the conclusions by other scholars that teenage youth do not want to be monitored by parents as much. It also aligns with the demonstrated youth understandings of privacy and security as being choice-based.

Extant literature on parental influence does suggest that conversation and communication are also important ways that parents influence their children's knowledge and behavior, with multiple studies concluding that "internet parenting is best achieved through an open communication style and through making connections with children" ([46][48][53]). Unfortunately, parents experience challenges with communicating with their children about OPS topics. Some parents feel that their children are too young to understand or exercise protective OPS behaviors, and admit that cybersecurity conversations at home are not common ([27][40][64][67]). Other parents have noted feeling like their own understandings are not strong enough to know how to protect their children ([15][32][66]). In these instances, especially with older youth, it may be difficult for parents to make meaningful contributions to their children's knowledge [66].

In summary, existing research on youth online privacy and security knowledge suggests that they have some understanding of these terms, but may not always put this knowledge into practice. In this literature, however, previous studies have focused on either online privacy or online security separately without differentiating between the terms. Additionally, past studies tend to examine a narrow age range of youth, and/or are tied to specific knowledge interventions. Our study aims to contribute to this field by investigating privacy and security knowledge in tandem (and thus exploring if youth can differentiate between the two concepts) and studying a broader age range of youth in order to compare knowledge across grade bands. We also seek to better understand youth knowledge *in situ* as opposed to in response to a learning task. Further, we aim to investigate youth knowledge alongside parental knowledge and understanding because of the important role that parents can play in shaping youth's knowledge and behavior development.

3. Methods

To answer this study's research questions about what children know about OPS and how parents attempt to influence that knowledge, we conducted a qualitative study consisting of pre-interview questionnaires and semi-structured interviews with 40 youth/parent dyads in spring 2021.

3.1. Recruitment and Participants

This study was approved by the Institutional Review Board (IRB) of the National Institute of Standards and Technology. Parent/child dyads for this study were recruited by a contracting research firm that used a preexisting user database; eligible parents self-elected themselves and their child for participation. A total of 40 youth/parent dyads from across the United States participated. These dyads included 4 youth from each grade from 3rd-12th grades and one of their parents, resulting in 12 elementary school (ES; 3rd-5th grades, 8 to 11 years old), 12 middle school (MS; 6th-8th grades, 12 to 14 years old), 16 high school (HS; 9th-12 grades, 15 to 18 years old) participants, and 40 parents. Demographic information for each dyad can be found in the table in Appendix A.

3.2. Instruments

Data were collected using a pre-interview questionnaire and a semi-structured interview. The two instruments were designed to be mutually inclusive; the questionnaires collected demographic data and participants' basic descriptions and positions about online privacy and security and served as a pre-thinking exercise for participants for the interview, and the interviews allowed participants to expand upon and discuss their answers from the questionnaire with thoughts, examples, and personal narratives. The questionnaire language was scaffolded to suit participants' age and role, resulting in three different versions: one for youth in grades 3-5, one for youth in grades 6-12, and one for parents. All three questionnaires consisted of content sections with demographic questions, general technology use questions, OPS knowledge questions, and three online risk questions. The parent questionnaire was six questions longer because parents were asked about both themselves and their children.

The semi-structured interview protocols were also scaffolded to suit participants' ages and roles [1]. Youth participants were asked 11 anchor questions about their knowledge of and behavior surrounding online privacy, security, and risk. Parent participants were asked 9 anchor questions about both their own knowledge of online privacy, security, and risk, as well as how they view their child's knowledge and behavior surrounding these ideas.

Two members of the research team—one quantitative expert and one qualitative expert—created an initial draft of the data collection tools using the research questions and extant literature as a guide. From there, the content and quality of both tools were refined over four iterative steps: (1) review by a survey expert, (2) review by research colleagues and four K-12 teachers, (3) cognitive interviews with three youth (one elementary, one middle, and one high schooler) [7], and (4) pilot interviews with three youth/parent dyads [55]. After each step in this process, the data collection tools were refined based on feedback and pilot participant responses. The study instruments are included in Appendix B.

3.3. Procedure

All data collection occurred remotely over Zoom[3] and was audio-recorded for transcription. The youth/parent dyads signed informed consent and assent forms (for youth older than 12) and were briefed about the study together.

Following the study overview and verbal consent/assent process, parent and youth participants were interviewed separately in order to afford both parties—but particularly youth participants—the privacy needed to answer potentially sensitive questions about their online activities as openly and honestly as possible. All parents and youth were given the option to have youth participants interviewed with their parent in the room if they were more comfortable with this option. One

[3] Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products mentioned are necessarily the best available for the purpose.

youth participant and one parent participant selected this option, and the other 38 dyads were interviewed separately.

Each of the 40 data collection Zoom calls were scheduled for 90 minutes, and the first author conducted all 80 interviews for consistency. Participants were compensated for their time with cash gift cards: parents received $75 and youth received $25. Any personal identifiable information (such as name and location) unintentionally revealed during the interview was properly redacted and removed from the data. Each participant was assigned a unique alphanumeric identifier. The data collection process yielded 80 complete pre-interview questionnaires and 546 pages of single-spaced interview transcripts.

3.4. Data Analysis

The qualitative data analysis for this study proceeded across two cycles and was guided by methods outlined by Johnny Saldaña [47]. Cycle one contained both inductive and deductive coding resulting in 84 first-cycle codes. This initial code deck was used by the first and third author to code a random selection of nine full dyad transcripts using Nvivo coding software. The full research team then met to discuss and refine the code deck. This process was repeated three more times with different samples of three dyad transcripts in order to refine the code deck. The first and third author then used the fourth revision of the code deck to run an interrater reliability (IRR) agreement statistic, which returned a Cohen's Kappa (k) value of .74 indicating substantial interrater agreement [36]. All coding discrepancies were resolved through discussion with the full research team. Once the IRR statistic was calculated, the first and third author completed a final first-round coding pass of all 40 dyad transcripts.

After all first-round coding was complete, the research team read through the coding results individually, then met to discuss patterns and themes for each research question from a dyadic perspective. To do this, we used the constant comparative method as outlined in Boejie [6] and Williams-Reade and colleagues [61] as mentor processes for how to compare and contrast codes across different participants and dyads seeking patterns, similarities, and differences which could then be categorized and conceptualized. In doing so, we followed these steps: (1) comparison of data and coding within a single participant's interview, (2) comparison between interviews within the same group (all youth and then all parents), (3) comparison between different groups (all youth with all parents), (4) comparison in pairs at the dyad level (individual youth with their parent), and (5) comparison across all dyads. Finally, the first author performed a second cycle theming of the resulting data using the research questions as a frame. A table demonstrating an example of the coding process can be found in Appendix C.

4. Results

The results of this study are evidenced with direct quotes from participants and cited with an alphanumeric identifier. In the identifiers, the "Y" or "P" indicates "youth" or "parent," the number is the dyad code, and the ES/MS/HS indicates whether the youth participant of that dyad was an elementary (3rd-5th), middle (6th-8th), or high school (9th-12th) student.

4.1. RQ1: What do youth know about OPS?

4.1.1 Youth online privacy descriptions

Youth across all grade bands in this study described online privacy as how one protects personal and important information, and often did so in interpersonal terms. In these descriptions, "information" primarily meant personal details such as full name, location, age, passwords, and financial information, and the goal was to keep it from being accessed by strangers, hackers, and other unwanted third parties. Youth described online privacy as a way to "have your independence" (Y03MS), "be safe" (Y06ES), and keep someone from "knowing your own business without you telling them" (Y22HS). The 40 youth also unanimously agreed that online privacy is important.

MS and HS youth also spoke about their online information privacy agentively, positioning it as something over which they had some control. For example, when Y22HS was explaining what he meant by preventing people from "knowing your own business without you telling them," he clarified that "a lot of [sketchy websites or skilled hackers] probably ask for credit card information or an email address or a phone number…the worst thing people can do is to give out information that's not necessarily needed." In this explanation, he positioned the online user as having the choice to either tell/give or not tell/give their information. Through such choices, older youth position online information privacy not as something simply afforded to a person, but instead as an idea that is always under construction and dependent upon an ongoing series of choices.

There was also a recognition across age groups that online privacy is contextual, and that within certain contexts a person can choose how much privacy they want to have. Games and social media served as important examples of this point; for instance, Y21MS explained that she chose to have a private TikTok account because "if I posted a video, I wouldn't want it blowing up to the point where it has a million [views]…it would be overwhelming," but that public accounts are the right choice for some people. Of the youth that discussed social media, all opted for private pages on platforms like Instagram and Pinterest, or stated a preference for apps like Snapchat that require a user to add "friends" before those friends can view shared content.

Finally, youth descriptions and examples of online privacy featured trust and feelings about security as central components for making good online privacy choices. Having a sense for which people and which websites are trustworthy—and, more frequently, which ones are *un*trustworthy—emerged as a way that youth believed they could keep themselves and their information private. For example, Y12ES advised that "no one really that you don't trust should know your private information." The most cited untrustworthy entities were strangers (writ large), hackers, and advertisements or pop-ups.

In terms of *why* they felt online privacy was important, responses overwhelmingly included the consequences of "being hacked and having your information stolen" (Y02MS), having someone "get into your bank account and take your money" (Y10ES), "identity theft" (Y22HS), and having sensitive information like "photos get(ting) leaked, and then it's extremely hard to get those photos off the web…that can affect your online and personal life" (Y27HS). HS youth were more likely to only cite virtual consequences of poor privacy choices like data theft and hacking by "the people that are good with computers" (Y39HS), while ES and MS youth were also frequently concerned about in-person consequences like kidnapping (Y18ES) and people who "could potentially steal from you and come over and rob [you]" (Y33MS).

4.1.2 Youth online security descriptions

Many youths described the online security by giving examples of choices that can be made to either increase or decrease security. Specifically, youth overwhelmingly mentioned good password behavior like making sure "all my passwords aren't the same" (Y21MS), setting "strong passwords" (Y14ES), and not "shar(ing) my passwords and stuff" (Y34HS), as well as broader device and browsing choices like using "a secure network" (Y04HS) and only clicking on "secure websites" (Y03MS). MS and HS youth also noted using certain technologies—like virtual private networks (VPN) and firewalls—to help maintain their online security.

To determine which websites were secure, youth sometimes cited concrete evidence like looking "in the left corner where it has the website link there's usually a green lock" (Y12ES), but also sometimes mentioned relying on simply "feel[ing] like I'm set to just know that I made the right choice" (Y32MS). Some youth also described feeling confident in their online security behavior because they had not (yet) experienced any negative consequences, like Y27(HS) who explained that she knew she was secure online because she "[hadn't] had my information leaked, [or] had any photos leaked."

Across grade bands, online security was described as a way to help ensure online privacy and protect against outside threats, specifically hackers and viruses. There was, however, a grade band difference in how much immediate, personal control youth felt that they had over their online security: youth in ES and lower MS were more likely to rely on parents and/or security software for security, while their upper MS and HS counterparts relied more on themselves and their ongoing choices. For example, Y09ES noted that before downloading apps "I always ask my dad first to see if maybe I could accidentally download a virus or something," While Y34HS reported feeling secure because he used "safe apps and…won't share my passwords."

4.1.3 Youth OPS understandings

While youth's OPS understandings in this study shared many characteristics, there was a difference between youth's privacy and security knowledge, with youth providing more extended and detailed descriptions of *online privacy*. Youth across grade bands were more likely to say things like "I know more with privacy than security" (Y31MS), or to have less depth in their security knowledge, like participant Y10ES who knew "you could add extra security to your device," but could not give an example of how. That being said, most of the youth *were* able to at least differentiate between "online privacy" and "online security," often using the idea of "privacy" in their descriptions of "security," but rarely the other way around. This suggests a specific (rather than random or conflated) understanding about the relationship between the two terms: that good security choices help ensure "that other people are not doing things that could potentially harm you or your privacy" (Y02MS).

Further, outsiders were cited as the biggest threat to both online privacy and online security. However, the nature of the threat was described slightly differently across the terms. With online privacy, youth described the threat as losing anonymity and, along with it, security, while with online security, youth described the threat as having information stolen. This understanding of threat seemed to also translate into an understanding of the role of agency.

The 40 youth in this study described being able to make good and bad choices that could either increase or decrease both their OPS. However, when it came to privacy, these choices were more often described as optional, ongoing, and existing on a spectrum, whereas with security the choices were described as more necessary, one-time in nature, and clear cut. For example, participant Y37HS referred to social media to discuss both her privacy and security choices, but in different ways. When talking about privacy, she described "only letting people that you know and that you are comfortable with follow you, and [being] aware of what you're posting," which are both ongoing efforts. However, she later mentioned making the more singular choice to maintain private social media accounts because "it's more secure."

Understanding OPS as being agentive choices as opposed to hard and fast rules held important implications for the youth, particularly surrounding the idea of calculated risks. Youth across grade bands in this study reported knowing about poor OPS choices, including making weak passwords, talking to strangers, illegally streaming content, and visiting questionable websites. However, the youth—in particular the MS and HS youth—were still making these choices anyways after deciding that either the consequences were low, the reward was worth the risk, or both. For example, participant Y39HS admitted knowing that "pirating NBA basketball streams that go through lots of different ads and [involve] clicking off and stuff" was a "very, very bad" choice, but that he consistently chose to do it anyways because "it's the only way I can watch the games." Such descriptions of calculated risks highlighted a particular sort of self-aware confidence shared by most of the youth: in the pre-interview questionnaire, only about one-third of youth participants (30%) said they knew "a lot" about online privacy, with that number dropping to 10% (4 participants) saying the same about online security (see Appendix A for youth self-reported knowledge levels). However, only 3 participants (7.5%) admitted that they do not believe they use their devices securely, while 79.5% (29 participants) stated that they always use their devices securely. This apparent contradiction was summarized beautifully by participant Y27HS. When asked why she chose "a Moderate amount" for the questionnaire questions asking how much participants felt they knew about OPS, she replied: "I feel like I know enough. I might not know a lot, but I think I know enough of how to keep myself safe online."

4.2. RQ2: How do parents understand the role of OPS in youth's lives?

Regardless of how parents viewed OPS in their own lives—which was varied—they unanimously agreed that these concepts were important for their children. For example, P11HS viewed her own online privacy as "a trade-off" in which "the more they [i.e., Google] know about me, the more relevant content I feel I'm going to get." However, when it came to her child, she noted that "especially for a kid… he has to be extra careful." Her sentiments were echoed by all 40 parents, who worried specifically about the consequences of their children's actions. These concerns led to an emphasis on talking about the consequences of youth's poor behavior as opposed to focusing on the benefits of good behavior.

The parents' understanding of consequences were shared evenly across both online privacy and online security, with the most frequently cited consequences being hacking, future social or professional repercussions, data loss or misuse, kidnapping or stalking, theft, seeing inappropriate content, and mental health repercussions. Parents of ES children were more likely to mention the consequence of their child seeing inappropriate content, while parents of MS children were more likely to worry about their child experiencing mental health repercussions from online social interactions.

While parents, themselves, were quite worried about the consequences of poor OPS choices, they generally did not feel that youth were similarly concerned. Parents across grade bands stated a belief that OPS *should* or *would* matter to their children at some point, but that right now "it's just not something that they're thinking about" (P27HS) or are "as interested in" (P02MS). Parents of ES and some MS children felt that youth in these grades were too young to "necessarily think about the ramifications" (P33MS), or did not have enough high-stakes accounts or developmental knowledge yet for privacy and security to truly matter. For example, P16ES shared that youth her child's age make choices "based off of their desires and things they want [without connecting] it to 'this could affect your real life.'" These parents were more likely than their HS counterparts to say that privacy and security mattered some now, but that "as they get older...they'll start to get it (P10ES). Parents of upper MS and HS youth described youth in these grades as being more impulsive and explained that "at their age, they just want to be accepted" (P21MS) and "don't think about the consequences down the road" (P37HS). This impulsiveness, parents explained, was the root of OPS mistakes.

Interestingly, parents' beliefs about "kids that age" were only sometimes reflected in their opinions of their own children, resulting in what we have dubbed the "good kid syndrome." Parents experiencing "good kid syndrome" were those who gave conflicting responses about what "youth" do versus what they believe their own child does, believing that their child was more secure than most other children. Examples of parents with "good kid syndrome" included P13MS who stated that "I'm sure there are all kinds of kids who give their name to people they don't know, maybe other whether large or small pieces of information that could personally identify them," but when asked about whether his child has done the same stated "I'm sure she has, knowingly or unknowingly, but I think hers are probably, in my view, I think they're probably average to below average versus other kids" (P13MS). Similarly, P27HS suggested that many teenagers "[connect] with people on social media that they don't know personally" but that her child was "one of the good ones…a level-headed kid."

4.3. RQ3: How do parents attempt to influence youth's privacy and security understandings?

4.3.1 How parents monitor their children's online activities

Parents used a variety of methods to physically monitor their children's device use in an attempt to ensure that their children were private and secure online. The monitoring methods that were specifically mentioned included restricting access to devices (i.e., at night or as punishment), limiting screen time, controlling in-device purchasing and browsing using parental monitoring applications, blocking websites or applications, observing device use, requiring devices to be used in a shared living space, and physically checking devices (i.e., looking at social media or browsing histories).

The parents who monitored their children ranged from passively monitoring using one method on an infrequent basis, to very actively monitoring, like P33MS who limited technology access, used parental controls, and observed use. Across all monitoring types, the amount and intensity of monitoring decreased as youth got older. This was found both within grade bands—HS parents reported decreasing monitoring behavior over time—as well as across all dyads, with ES parents reporting doing more monitoring than HS parents, and MS parents falling in between.

Parents of ES and MS youth were the most likely to rely on parental controls, but had complaints that parental controls were not nuanced enough, particularly for pre-teen youth who "kind of [fall] through the cracks…there's no in-between" (P18ES). Overall, despite the proliferation of device monitoring of all kinds, when we compared parents' monitoring choices with their children's understandings of OPS, we found no significant patterns between amount or type of monitoring and level of youth understanding.

4.3.2 How parents talk to their children

In addition to monitoring, many parents reported having conversations with their children about OPS. A majority of the conversations that parents described having were about the consequences of poor choices, and were reactionary in nature. For example, P30HS recalled having a conversation about talking with strangers online and security settings *after* her daughter and a friend "were playing Roblox and a weirdo, an adult male, decided to chat with them." Similarly, P02MS admitted talking more about online privacy than security with her daughter because "that's where I've seen the issue, honestly."

Parents who chose *not* to have conversations about OPS with their children felt that the knowledge was coming from elsewhere, like P22HS said she did not have OPS conversations with her son because "I think he's been given lessons about it in school." Technology was also cited as a reason to not need to have explicit conversations, like when P28HS explained that she "rel[ies] on a lot of websites that require a capital and a lowercase and a number [for passwords], so that kind of takes care of it," and P35HS reasoned that "if I have this [security] suite and I keep it up to date, that should generally protect him…I've not had a conversation with him."

Parents' decisions to have conversations about OPS dependent on their child's age. Parents of ES and MS youth most frequently reported either tailoring their conversations to their child's perceived technological understandings or holding off on the conversation altogether until their children are older. P10ES explained that she currently only has a "small amount" of conversations with her daughter "due to age and because she only has a tablet…but as [she] gets older and [she gets] more independent, of course, you need to have those conversations." Similarly, while P17ES made and stored all of her son's passwords for him at the time of interview, she noted that "sometime soon [he's] going to have to pick his own password for something…[and] then he'll probably listen and we'll discuss it."

Conversely, the parents of HS youth believed that their children either already know about online privacy or were old enough for the conversations to no longer be necessary. P11HS was one such mom, who described her son as "a little man," and noted that "we've had all those conversations, but it's been years. I honestly don't know what he knows at this point…because honestly we haven't had those conversations probably in three or four years." Interestingly this parent, as well as several of her peers who reported not talking to their children about these topics, overwhelmingly stated that they (the parents) were most responsible for their children's knowledge, while also admitting that they do not regularly (if ever) talk to their children about OPS.

Finally, the results of this study reveal that parents want to know more about OPS but are unsure how to do so. Of the parents who described not talking to their children about OPS at all, all but one self-reported knowing "little" about either online privacy, security, or both. One of these parents reflected that "this research has reminded me how little I know about OPS, and since my kids are young, it's my job to teach them" (P12ES). P31MS noted: "I hope that as a parent I can stay on top of all the changing online interactions…[but] I feel a bit overwhelmed at times regarding this topic." These comments, combined with the large number of parents who said they "want to learn more about this topic and how I can make better safety choices for me and my children" (P35HS) suggest that parents' perceived levels of knowledge may impact the amount and kind of conversations they choose to have with their children about OPS. This possibility is especially interesting considering only 4 parents in this study (10%) reported feeling like they know "a lot" about OPS.

4.3.3 The Influence of Parents on Children

Overall, the youth in this study with more nuanced descriptions and understandings of OPS had parents who reported having conversations with them instead of or in addition to the monitoring of device use. This finding held true regardless of the parents' self-reported levels of OPS knowledge (see Appendix A), of how confident they were in having the conversations, or of the strength of parents' own stated understandings. For example, when talking about having online security discussions with her son, P20MS explained that "we just basically talk to him about the fact that certain websites are inappropriate or even could give him a virus." She also noted that the conversations involved explanations and were "usually not just like 'oh we don't want you to,' we usually give him a reason why we don't want him to be on that and why that behavior is inappropriate" (P20MS). These conversations were directly reflected in the ways Y20MS talked about online security: he mentioned keeping information secure using VPNs and firewalls, avoiding pop-ups and dangerous websites that can cause viruses, noted that he runs security scans on his computer, and discussed the role of personal choice in a person's level of online security. He also identified the consequences of risky online behavior as including "leading you to something that's really inappropriate" and "giving your computer malware or a virus" (Y20MS).

By contrast, the youth—especially ES and MS aged youth—whose parents relied on physical monitoring in lieu of conversations could generally provide descriptions of OPS, but struggled to explain *why* OPS is important and to provide examples. For example, P26ES noted that she "monitor[s] [her son's] phone to the fifth power" and, when asked if they have conversations about privacy and security, replied yes. After replying yes, however, she proceeded to provide an example of hearing foul language during a video game at which time she "took his headphones and said, 'you can't play, just turn it off.'" Consequently, her fifth-grade son Y26ES described online privacy as "not to be bothered" online, and said he did not know what online security was.

With ES aged youth in particular, the parents who reported having conversations with their child had youth with more nuanced understandings. Conversely, elementary aged youth like Y26ES whose parents chose not to discuss OPS with them demonstrated lower levels of understanding and less nuanced descriptions. With HS participants, this gap disappeared: HS parents almost unanimously reported not having recent online privacy or security conversations with their children, but most HS youth still provided detailed descriptions and nuanced examples of both terms.

5. Discussion

Our study sought to learn more about youth's OPS knowledge, as well as how parents understand and attempt to influence that knowledge. It was unique in its design and purpose in two ways. First, we studied parent/youth dyads (as opposed to one population or the other) with a broader age range of participants (10 standard United States school grades–3rd to 12th), which allowed us to examine findings both within and across dyads and grade bands to look for interrelationships not able to be studied using other designs. Second, we were also curious about youth knowledge in general versus in response to specific learning interventions or experiences.

In terms of youth OPS knowledge, when asked to describe and give examples of OPS, the 40 youth in our study, regardless of age, were able to describe both terms, and were able to name examples and online choices that exemplified good and bad OPS behavior. Their descriptions and examples supported several preexisting findings about youth's OPS understandings, particularly that youth do know about, care about, and value these ideas [67]; and that there are often gaps between what youth say they know and the actions they take ([15][44]). Our study also supported existing findings about parents' understanding of their children's knowledge and attempts to influence that knowledge, namely that parents frequently choose device monitoring and physical or technical controls over conversations ([27][64]); often hold misguided understandings about youth's knowledge, including the idea that younger children are too young to understand or exercise protective practices[40]; and are concerned about their own knowledge not being strong enough to best support their children [15]. Our study's most compelling findings arose when examining youth and parent knowledge both within and across dyads and grade bands. Our study's greatest contribution to the ongoing investigation of youth OPS knowledge is our examination of the relationships between parent knowledge, parent OPS monitoring and education, and youth knowledge .

5.1. Parental Influence on Youth Understandings

What the 40 parents in this study understood about their children's OPS knowledge can be summarized into three broad categories: those who believed their children were too young to fully understand or care, those who believed their children were "good kids" who wouldn't get into trouble, and those who felt like their children already knew enough to make good choices. All three beliefs, however, generated similar parental influence responses: an emphasis on passive monitoring (i.e., parental controls and device monitoring), or conversations that mostly centered on consequences of poor online choices. We also found, however, that parental conversations—either alone or in conjunction with monitoring—may be more effective at establishing stronger youth understandings than device monitoring alone.

These conflicting factors—along with the fact that the parents of younger youth frequently mentioned that conversations with their children would happen "later," while parents of older youth noted that such conversations are no longer necessary—collectively raise the question of when the magic time frame for conversations with children about OPS is, and if these conversations ever wind up consistently happening at all. On one hand, younger youth whose parents did more passive monitoring than conversational engagement had less nuanced privacy and security understandings. On the other hand, high school youth had more complete and nuanced understandings regardless of the methods of parental influence. This suggests that at some point, children begin gaining OPS knowledge from sources outside their parents that help round out their understandings. However, up until that point, parental influence has the potential to make a meaningful difference in youth OPS knowledge and behavior, and the type of parental influence matters.

Further, youth in this study understood OPS as agentive and user-influenced, suggesting that conversations with youth about decision-making surrounding the use and sharing of information and data online may be more important than more prescriptive approaches to building understanding like defining rules or pre-setting controls. If youth understand OPS as elements of their technical selves that require risk calculation and choice, having conversations about how to weigh such decisions and make good choices—as well as the potential consequences of choosing to engage in less private and less secure choices—is likely more helpful than monitoring. As youth grow and their online activities diversify, they will be increasingly faced with choices concerning their OPS and need to be armed with the knowledge and skills to make these choices, and parents simply cannot always be watching. The youth and parents in our study indicate that parental conversations with youth either in addition to other forms of monitoring or as the sole form of monitoring, alone, is likely a better approach. Further, contrary to parental belief, there is no such thing as "too early" for these conversations because, as these 40 youth indicate, youth of *all* ages understand the importance of OPS and are prepared to think about how to protect themselves online.

5.2. Implications

5.2.1 Implications for Parents

The primary takeaway from this study for parents is straightforward: talk about OPS choices with children, and begin doing so in the elementary years as soon as youth are given access to devices. Our study suggests that parents do not have to be experts—or even be incredibly confident in their own OPS knowledge—for these conversations to be successful. Rather, especially given the ever-evolving nature of these topics [18], parents can co-construct and continue to learn alongside their youth via conversations about OPS choices and behaviors versus feeling like they need to be OPS experts to be helpful. This idea of co-constructing knowledge could help overcome the gaps in knowledge that both youth *and* parents have when it comes to OPS ([8][66]), as well as prepare youth to be informed decision-makers when making OPS choices they feel they are responsible for.

5.2.2 Implications for Technology Providers

Like other literature examining parent and youth understandings of privacy, our study supported that both youth and parents think about online security and especially online privacy more at the interpersonal levels and less at the commercial and institutional levels [33]. It also revealed through a social learning lens that by middle school, most youth may be getting as much or more of their information about OPS from outside the home, including from technology tools, devices, applications, and services. This means that technology providers have the opportunity and possibly even the responsibility to support youth knowledge, especially when it comes to understandings like how data is collected, stored, and tracked. These providers might consider making more proactive, outcome-based tools to support parents instead of monitoring-based ones, or creating more educational tools to teach young users about OPS choices and choice-outcomes. Similarly, providers might consider creating tools for passive-monitoring parents to help them supplement their current strategies with conversational approaches.

5.2.3 Implications for Future Research

Extant research and literature tend to either conflate online privacy and security, or to specifically investigate one of the terms in isolation from the other. Our study—which investigated both terms separately from each other—reveals that both parents and youth of all ages do understand these terms as interrelated but distinct, and that youth have more knowledge and exposure to online privacy than online security. Future user-centered research should further explore youth's interconnected understandings to explore how youth use their OPS knowledge in conjunction to stay secure and private online instead of as separate or singular entities. Further, our study showed that especially older youth approach OPS from an agentive perspective, and intentionally make choices to engage or not engage in private and secure behavior. More research investigating the nature of these choices and how youth make them could go a long way in continuing to support our understanding of youth habits.

Finally, our study preliminarily reveals that the when, how, and what of parent conversations about OPS has the power to influence youth understandings, especially with youth in elementary and middle school. Further qualitative explorations into the kinds of conversations that parents have could help build a better understanding of exemplary characteristics of such conversations. More dyadic studies are a recommended approach to this work because of their unique ability to examine both parent and youth actions, perspectives, and resulting knowledge. Importantly, work is needed to understand how parents and youth feel about the extent and type of influence each have on understandings of OSP.

6. Positionality and Limitations

The positionality of the authors in this study is important to note. The first author is an educator and has worked with youth for over a decade and the second author is a parent, and these positionalities and related experiences explicitly surfaced throughout data analysis discussions. The influences of these positionalities were mitigated by a rigorous data analysis process, as well as full-team data analysis discussions during which individual assumptions surfaced and were identified and discussed by the research team, including the third author who was neither a parent nor a teacher.

Additionally, this study had several limitations. First, because of the COVID-19 pandemic, interviews happened via video platform. This meant that, although we requested that individual participants complete the interview privately, there was a nonzero chance of youth/parent participants overhearing and influencing each other's responses or responding with the possibility of being overheard by others. Further, common limitations for qualitative data in general applied to our study, including the possibility of biases in participants' self-reports of behavior (e.g. optimism bias [48]), and potential order effects by asking about online privacy first and security second [39].

Finally, our study was limited by its cross-sectional design focusing only on parents and youth at one point in time. This study was not longitudinal, meaning we could compare dyads within and across age groups, but could not examine the progression of parental influence and youth knowledge of the same dyads over time. Further, our theoretical approach requires an understanding that youth knowledge is impacted by a variety of factors including things like school and peers, but we scoped the study specifically to the influence of parents.

Each of these design limitations offers important potential directions for future research, such as focusing on longitudinal data and/or more holistic approaches to understanding how a variety of factors are influencing youth at different ages.

7. Conclusion

In conclusion, this study showed that the 40 3rd-12th grade youth we interviewed had at least basic—and at times nuanced and interconnected—OPS knowledge. Further, they viewed these topics as important and were aware that participation in the online world includes frequent opportunities to make privacy- and security-related choices. For these youth, particularly the younger youth in elementary and middle school, parents were influential contributors to this knowledge and these choices, and had the power and influence to help their children be more private and secure online. For these 40 parents, the most effective strategy for influencing their children's knowledge and understandings was through conversations and learning alongside their children, even when they thought their children might not be interested or old enough to fully "get it."

Continued learning about what young users know about OPS is an important step in the ongoing process of discovering how, when, and where to teach them this knowledge. The younger that youth can learn to flexibly practice strong OPS practices, the better prepared they will be to keep themselves secure online. Further, because we know that parents play an active and important role in this learning [4], the more we can help prepare parents to have constructive conversations about OPS with their children the better.

References

[1] Fenio Annasingh and Thomas Veli. An investigation into risks awareness and e-safety needs of children on the internet. *Interactive Technology and Smart Education*, vol. 13, no. 2, pp. 147-165, 2016.

[2] Lioness Ayres. Semi-structured interview. *The SAGE encyclopedia of qualitative research methods*, vol. 1, pp. 810-811, 2008.

[3] Karla Badillo-Urquiola, Yaxing Yao, Oshrat Ayalon, Bart Knijnenurg, Xinru Page, Eran Toch, Yang Wang, and Pamela J. Wisniewski. Privacy in Context: Critically Engaging with theory to guide privacy research and design. In *Companion of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing,* 2018, October, pp. 425-431.

[4] Albert Bandura. *Social Learning Theory,* New York: General Learning Press, 1977.

[5] Stacy Black, Rezvan Joshaghani, Dhanush Kumar Ratakonda, Hoda Mehrpouyan, and Jerry Alan Fails. Anon what what? Children's Understanding of the Language of Privacy. In *Proceedings of the 18th ACM International Conference on Interaction Design and Children*, pp. 439-445, 2019.

[6] Hennie Boeije. A purposeful approach to the constant comparative method in the analysis of qualitative interviews. *Quality and quantity,* vol. *36,* no. 4, pp. 391-409, 2002.

[7] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, vol. 4, no. 3, pp. 340-347, 2013.

[8] Eva Irene Brooks and Anders Kalsgaard Moeller. Children's perceptions and concerns of online privacy. *Extended Abstracts of the Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts*, pp. 357-362, 2019.

[9] Sangmi Chai, Sharmistha Bagchi-Sen, Claudia Morrell, H. Raghav Rao, and Shambhu J. Upadhyaya. Internet and online information privacy: An exploratory study of preteens and early teens. *IEEE Transactions on Professional Communication*, vo. 52, no. 2, pp. 167-182, 2009.

[10] Hui-Lien Chou, Yih-Lan Liu, and Chien Chou. Privacy behavior profiles of underage Facebook users. *Computers & Education,* vol.128, pp. 473-485, 2019.

[11] Merijke Coenraad, Anthony Pellicone, Diane Jass Ketelhut, Michel Cukier, Jan Plane, and David

Weintrop. Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games. *Simulation & Gaming*, vol. 51, no. 5, pp. 586-611, 2020.

[12] Katie Davis, and Carrie James. Tweens' conceptions of privacy online: Implications for educators. *Learning, Media and Technology*, vol. 38, no. 1, pp. 4-25, 2013.

[13] John Dempsey, Gavin Sim, and Brendan Cassidy. Designing for GDPR-investigating children's understanding of privacy: A survey approach. *32nd Human Computer Interaction Conference,* Belfast, Ireland, 2018.

[14] Laura M. Desimone, and Kerstin Carlson Le Floch. Are we asking the right questions? Using cognitive interviews to improve surveys in education research. *Educational evaluation and policy analysis*, vol. 26, no. 1, pp. 1-22, 2004.

[15] Laurien Desimpelaere, Liselot Hudders, and Dieneke Van de Sompel. Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in human behavior*, vol. 110, no. 106382, 2020.

[16] Sonya Corbin Dwyer and Jennifer L. Buckle. The space between: On being an insider-outsider in qualitative research. *International journal of qualitative methods* vol. 8, no. 1, pp. 54-63, 2009.

[17] Yang Feng and Wenjing Xie. Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. *Computers in Human Behavior,* vol. 33, pp. 153-162, 2014

[18] David Finkelhor, Lisa Jones, and Kimberly Mitchell. Teaching privacy: A flawed strategy for children's online safety. *Child Abuse & Neglect* vol. 117, no. 105064, 2021.

[19] Alexa K. Fox and Mariea Grubbs Hoy. Smart devices, smart decisions? Implications of parents' sharenting for children's online privacy: An investigation of mothers. *Journal of Public Policy & Marketing*, vol. 38, no. 4, pp. 414-432, 2019.

[20] Steven Furnell and Emily Collins.S. Cyber security: what are we talking about? *Computer Fraud & Security*, vol. 2021, no. 7, pp. 6–11, 2021, doi: https://doi.org/10.1016/S1361-3723(21)00073-7.

[21] Steven Furnell, Rawan Esmael, Weining Yang, and Ninghui Li. Enhancing security behaviour by supporting the user. *Computers & Security,* vol. 75, pp. 1-9, 2018.

[22] Simon L. Jones, Emily IM Collins, Ana Levordashka, Kate Muir, and Adam Joinson. What is 'Cyber Security'? Differential Language of Cyber Security Across the Lifespan. in *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–6. Doi: 10.1145/3290607.3312786

[23] Flavius Kehr, Tobias Kowatsch, Daniel Wentzel, and Elgar Fleisch. Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, vol. 25, no. 6, pp. 607-635, 2015.

[24] Beeban Kidron, Angharad Rudkin, Miranda Wolpert, Joanna R. Adler, Andrew K. Przybylski, Elvira Perez Vallejos, Henrietta Bowden-Jones, Joshua J. Chauvin, Kathryn L. Mills, Marina Jirotka, and Julian Childs. *Digital Childhood: Addressing Childhood Development Milestones in the Digital Environment,* Technical Report, 5Rights, 2017.

[25] Abdullah Konak. Experiential learning builds cybersecurity self-efficacy in K-12 students. *Journal of Cybersecurity Education, Research and Practice,* no. 2018(1), p. 6, 2018.

[26] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 'No Telling Passcodes Out Because They're Private' Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction* 1, no. CSCW, pp. 1-21, 2017.

[27] Priya Kumar, Jessica Vitak, Marshini Chetty, Tamara L. Clegg, Jonathan Yang, Brenna McNally, and Elizabeth Bonsignore. Co-designing online privacy-related games and stories with children. In *Proceedings of the 17th ACM conference on interaction design and children*, pp. 67-79, 2018.

[28] J. Richard Landis, and Gary G. Koch. The measurement of observer agreement for categorical data. *Biometrics*, pp. 159-174, 1977.

[29] Sonia Livingstone. Children's privacy online: experimenting with boundaries within and beyond the family. In R. Kraut, M. Brynin, and S. Kiesler (eds.) *Computers, Phones, and the Internet: Domesticating Information Technology,* Human technology interaction series, Oxford University Press, New York, pp. 145-167, 2006.

[30] Sonia Livingstone, Giovanna Mascheroni, Michael Dreier, Stephane Chaudron, and Kaat Lagae. *How parents of young children manage digital devices at home: The role of income, education and parental style*, London: EU Kids Online, LSE, 2015.

[31] Sonia Livingstone, Giovanna Mascheroni, and Elisabeth Staksrud. European research on children's internet use:

Assessing the past and anticipating the future," *New media & society*, vol. 20, no. 3, pp. 1103-1122, 2018.

[32] Sonia Livingstone and Kjartan Olafsson. When do parents think their child is ready to use the internet independently? *Parenting for a digital future: Survey Report 2, Department of Media and Communications*, the London School of Economics and Political Science, London, UK, 2018.

[33] Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri. *Children's data and privacy online: growing up in a digital age: an evidence review*, London School of Economics and Political Science, Department of Media and Communications, London, UK, 2019.

[34] Paweena Manotipya and Kambiz Ghazinour. Children's Online Privacy from Parents' Perspective. *Procedia Computer Science,* vol. 177, pp. 178-185, 2020.

[35] Craig McDonald-Brown, Kumar Laxman, and John Hope. An exploration of the contexts, challenges and competencies of pre-teenage children on the internet. *International Journal of Technology Enhanced Learning*, vol. 8, no. 1, pp. 1-25, 2016.

[36] Mary L. McHugh. Interrater reliability: the kappa statistic. *Biochemia medica,* vol. 22, no. 3, pp. 276-282, 2012.

[37] Ingrida Milkaite, Ralf De Wolf, Eva Lievens, Tom De Leyn, and Marijn Martens. Children's reflections on privacy and the protection of their personal data: A child-centric approach to data protection information formats. *Children and Youth Services Review,* vol. 129, 2021.

[38] Tehila Minkus, Kelvin Liu, and Keith W. Ross. Children seen but not heard: When parents compromise children's online privacy. In *Proceedings of the 24th International Conference on World Wide Web*, pp. 776-786, 2015.

[39] David W. Moore. Measuring new types of question-order effects: Additive and subtractive. *The Public Opinion Quarterly*, vol. 66, no. 1, pp.80-91, 2002.

[40] James Nicholson, Julia Terry, Helen Beckett, and Pardeep Kumar. Understanding Young People's Experiences of Cybersecurity. *European Symposium on Usable Security,* pp. 200-210, 2021.

[41] Joshua C. Nwokeji, Richard Matovu, and Bharat Rawal. The use of Gamification to Teach Cybersecurity Awareness in information systems. In *Proceedings of the 2020 AIS SIGED International Conference on Information Systems Education and Research,* no. 29, 2020.

[42] Sean Oesch, Ruba Abu-Salma, Oumar Diallo, Juliane Krämer, James Simmons, Justin Wu, and Scott Ruoti. User Perceptions of Security and Privacy for Group Chat: A Survey of Users in the US and UK. *Annual Computer Security Applications Conference*. Association for Computing Machinery, Austin, USA, pp. 234–248, 2020. Doi: 10.1145/3427228.3427275.

[43] Gwenn Schurgin O'Keeffe, and Kathleen Clarke-Pearson. The impact of social media on children, adolescents, and families. *Pediatrics*, vol. 127, no. 4, pp. 800-804, 2011.

[44] Luci Pangrazio and Neil Selwyn. 'My Data, My Bad...' Young People's Personal Data Understandings and (Counter) Practices. In *Proceedings of the 8th International Conference on Social Media & Society*, pp. 1-5, 2017.

[45] Jean Piaget. Intellectual evolution from adolescence to adulthood. *Human development*, vol. 15, no. 1, 1-12, 1972.

[46] Farzana Quayyum, Daniela S. Cruzes, and Letizia Jaccheri. Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, vol. 30, p. 100343, 2021.

[47] Johnny Saldaña. *The coding manual for qualitative researchers,* 3rd ed., Sage, 2016.

[48] Tali Sharot. The optimism bias. *Current biology*, vol. 21, 23, pp.941-945, 2011.

[49] Wonsun Shin, and Hyunjin Kang. Adolescents' privacy concerns and information disclosure online: The role of parents and the Internet. *Computers in Human Behavior,* vol. 54, pp. 114-123, 2016.

[50] Kingkarn Sookhanaphibarn and Worawat Choensawat. Educational Games for Cybersecurity Awareness. *2020 IEEE 9th Global Conference on Consumer Electronics (GCCE)*, pp. 424-428, IEEE, 2020.

[51] M. Stoilova, S. Livingstone, S., and R. Nandagiri, *Children's data and privacy online: Growing up in a digital age, Research findings,* London: London School of Economics and Political Science, 2019.

[52] Mariya Stoilova, Sonia Livingstone, and Rishita Nandagiri. Digital by default: Children's capacity to understand and manage online data and privacy. *Media and Communication*, vol. 8, no. 4, pp. 197-207, 2020.

[53] Katrien Symons, Koen Ponnet, Michel Walrave, and Wannes Heirman. A qualitative study into parental mediation of adolescents' internet use. *Computers in Human Behavior,* vol. 73, pp. 423-432, 2017.

[54] Monika Sziron and Elisabeth Hildt. Digital media, the right to an open future, and children 0–5. *Frontiers in Psychology*, 2137, 2018.

[55] Edwin Van Teijlingen and Vanora Hundley. The importance of pilot studies. *Social research update*, vol. 35, no. 4, pp. 49-59, 2010.

[56] Mary Theofanos, Yee-Yin Choong, and Olivia Murphy. 'Passwords Keep Me Safe'–Understanding What Children Think about Passwords. *30th USENIX Security Symposium (USENIX Security 21)*, pp. 19-35. 2021.

[57] Sreenivas Sremath Tirumala, Abdolhossein Sarrafzadeh, and Paul Pang. A Survey on Internet Usage and Cybersecurity Awareness in Students. *14th Annual Conference on Privacy, Security and Trust (PST),* 2016.

[58] U.S. Department of Education, National Center for Education Statistics. Children's Internet Access at Home. [Online], *The Condition of Education 2021* (NCES 2021-144), 2021, Available: https://nces.ed.gov/programs/coe/indicator/cch

[59] Martin Valcke, Tammy Schellens, Hilde Van Keer, and Marjan Gerarts. Primary school children's safe and unsafe use of the Internet at home and at school: An exploratory study. *Computers in human behavior*, vol. 23, no. 6, pp. 2838-2850, 2007.

[60] José Van Dijck. *The culture of connectivity: A critical history of social media*. Oxford University Press, 2013.

[61] Jacqueline M. Williams-Reade, Daniel Tapanes, Brian J. Distelberg, and Susanne Montgomery. Pediatric Chronic Illness Management: A Qualitative dyadic analysis of adolescent patient and parent illness narratives. *Journal of marital and family therapy*, vol. *46*, no. 1, pp. 135-148, 2020.

[62] Christine Ee Ling Yap and Jung-Joo Lee. 'Phone apps know a lot about you!' educating early adolescents about informational privacy through a phygital interactive book. *Proceedings of the Interaction Design and Children Conference*, pp. 49-62, 2020.

[63] Ramazan Yilmaz, F. Gizem Karaoglan Yilmaz, H. Tugba Özturk, and Tugra Karademir. Examining secondary school students' safe computer and internet usage awareness: an example from Bartın province. *Pegem Journal of Education and Instruction,* vol. 7, no. 1, pp. 83-114, 2017.

[64] Leah Zhang-Kennedy, Christine Mekhail, Yomna Abdelaziz, and Sonia Chiasson. 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*, pp. 388-399, 2016.

[65] Leah Zhang-Kennedy, Yomna Abdelaziz, and Sonia Chiasson. Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. *International Journal of Child-Computer Interaction,* vol. 13, pp.10-18, 2017.

[66] Jun Zhao. Are Children Well-Supported by Their Parents Concerning Online Privacy Risks, and Who Supports the Parents? *arXiv preprint arXiv:1809.10944*, 2018.

[67] Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. I make up a silly name' Understanding Children's Perception of Privacy Risks Online. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pp. 1-13, 2019.

[68] Zahidah Zulkifli, Nurul Nuha Abdul Molok, Nurul Hayani Abd Rahim, and Shuhaili Talib. Cyber Security Awareness Among Secondary School Students In Malaysia. *Journal of Information Systems and Digital Technologies,* vol. 2, no. 2, pp. 28-41, 2020.

Appendix A. Demographics and self-reported OPS knowledge responses

Dyad ID	Youth (Grade)	Youth Self-Rated Knowledge		Youth Self-Reported whether always using electronic devices securely	Parent (Age)	Parent Self-Rated Knowledge		Parent Perception on whether the child always uses electronic devices securely
		Privacy	Security			Privacy	Security	
D01	Boy (8th)	A lot	A lot	Yes	Mom (48)	Moderate	Moderate	Yes
D02	Girl (6th)	Moderate	Moderate	Yes	Mom (48)	Moderate	Moderate	No
D03	Boy (6th)	Moderate	Moderate	Yes	Mom (38)	Moderate	Moderate	Yes
D04	Girl (9th)	Little	Little	Not sure	Mom (44)	Moderate	Moderate	No
D05	Boy (12th)	Little	Little	Yes	Mom (37)	Moderate	Moderate	Yes
D06	Boy (3rd)	A lot	A lot	Yes	Mom (34)	Moderate	Moderate	Yes
D07	Boy (4th)	Moderate	Little	Yes	Mom (39)	Little	Little	Yes
D08	Boy (3rd)	Little	Little	Not sure	Mom (37)	Moderate	Moderate	Not sure
D09	Girl (4th)	Moderate	Little	Yes	Dad (35)	A lot	A lot	No
D10	Girl (3rd)	Little	Little	Yes	Mom (31)	Moderate	Moderate	Yes
D11	Boy (10th)	Moderate	Moderate	No	Mom (52)	Moderate	Moderate	Not sure
D12	Girl (5th)	Moderate	Moderate	Yes	Mom (50)	Little	Little	No
D13	Girl (7th)	Moderate	Moderate	Yes	Dad (46)	Moderate	Moderate	No
D14	Boy (4th)	A lot	Moderate	Yes	Mom (52)	Moderate	Moderate	Yes
D15	Girl (5th)	Moderate	A lot	Yes	Mom (34)	Moderate	Moderate	Not sure
D16	Girl (4th)	A lot	Moderate	Yes	Mom (39)	Moderate	Little	No
D17	Boy (3rd)	-	-	Not sure	Dad (41)	Moderate	Moderate	No
D18	Girl (5th)	A lot	Moderate	Yes	Mom (52)	Moderate	Moderate	No
D19	Boy (7th)	A lot	Moderate	Yes	Dad (42)	Moderate	Moderate	Not sure
D20	Boy (8th)	A lot	Moderate	Yes	Mom (39)	Moderate	Moderate	No
D21	Girl (7th)	Little	Little	Yes	Mom (36)	A lot	A lot	No
D22	Boy (11th)	Moderate	Moderate	Yes	Mom (48)	Little	Little	Not sure
D23	Boy (9th)	A lot	Moderate	Yes	Mom (47)	Moderate	Moderate	No
D24	Boy (11th)	Moderate	-	Yes	Mom (36)	Moderate	Moderate	No
D25	Girl (8th)	Moderate	Moderate	Yes	Mom (33)	Moderate	Little	No
D26	Boy (5th)	Moderate	Little	No	Mom (42)	A lot	A lot	Yes
D27	Girl (11th)	Moderate	Moderate	Yes	Mom (39)	Moderate	Moderate	Not sure
D28	Girl (12th)	Moderate	Moderate	Not sure	Mom (41)	Little	Little	Not sure
D29	Boy (6th)	Little	Moderate	Not sure	Mom (34)	Little	Little	Not sure
D30	Girl (9th)	A lot	A lot	Yes	Mom (51)	A lot	A lot	No
D31	Girl (8th)	A lot	Little	Yes	Mom (45)	Moderate	Moderate	Yes
D32	Girl (6th)	A lot	Moderate	Yes	Mom (44)	Moderate	Moderate	Not sure
D33	Boy (7th)	Moderate	Little	Yes	Mom (50)	Moderate	Moderate	Yes
D34	Boy (10th)	Moderate	Little	Yes	Dad (51)	Moderate	Moderate	Not sure
D35	Boy (9th)	Moderate	Moderate	Not sure	Mom (42)	Moderate	Moderate	No
D36	Girl (12th)	Moderate	Moderate	Not sure	Mom (44)	Little	Little	Not sure
D37	Girl (10th)	A lot	Moderate	Yes	Mom (51)	Little	Little	No
D38	Girl (11th)	Moderate	Moderate	Not sure	Mom (48)	Little	Little	Yes
D39	Boy (12th)	Moderate	Little	No	Mom (39)	Little	Little	Not sure
D40	Boy (9th)	-	-	-	Mom (35)	Moderate	Little	Yes

Appendix B. Study Instruments

Pre-interview Questionnaire – Youth

1. Choose your gender: [radio buttons: *Boy/Girl* for ES; *Male/Female* for MS/HS]
2. How old are you? [entry field] (in years)
3. What is your grade? [drop-down list from 3rd to 12th]
4. Do you have a smartphone? [radio buttons: *Yes, my own/Yes, I share one with someone else/No*]
   [If the answer to Q4 is "No," then skip to Q5]
   4.1 How old were you when you first got a smartphone? [entry field] (in years)
   4.2 On average, how many hours a day do you spend on your smartphone? [entry field] (in hours)
5. Do you use a computer at home? (meaning a desktop, a laptop, or a tablet) [radio buttons: *Yes, my own/Yes, I share one with someone else/No*]
6. How would you define online privacy? [text area]
7. How much do you know about online privacy? [radio buttons: *A little/A middle amount/A lot* for ES; *Very little to nothing/A moderate amount/A lot* for MS/HS]
8. [ES] Who taught you about online privacy? [MS/HS] From whom did you learn about online privacy? [matrix with Yes/No options for each item below]
   Your parents or guardians; Brothers/Sisters for ES, *Siblings* for MS/HS]; *Other family members; Teachers/school; Friends; Yourself; Other*
9. How would you define online security? [text area]
10. How much do you know about online security? [radio buttons: *A little/A middle amount/A lot* for ES; *Very little to nothing/A moderate amount/A lot* for MS/HS]
11. [ES] Who taught you about online security? [MS/HS] From whom did you learn about online privacy? [matrix with Yes/No options for each item below]
    Your parents or guardians; Brothers/Sisters for ES, *Siblings* for MS/HS]; *Other family members; Teachers/school; Friends; Yourself; Other*
12. Do you think you always use your electronic device(s) securely? (meaning smartphone, desktop, laptop, tablet) [radio buttons: *Yes/No/I'm not sure*]
13. How would you define risky online behavior? [text area]
14. Have your parents/guardians spoken to you about risky online behaviors? [radio buttons: *Yes/No/I don't remember*]
15. Would you say you know more, the same, or less about technology than your parents/guardians? [radio buttons: *More/About the same/Less/I'm not sure*]

Semi-Structured Interview Scrip – Youth

1. Tell me about how you spend most of your time online.
2. I see you said you know [*response from questionnaire Q15*] about technology than your parents; can you explain this answer and why you said this?
3. (ES) Does anyone in your house watch or check in on what you do online? Does anyone control how much time you spend online? [If yes, who and how?] (MS/HS) Does anyone in your house monitor what you do online or how long you spend online? [If yes, who and how?]
4. I see you defined online privacy as [*response from questionnaire Q6*]. Do you think online privacy is important? [Why or why not?]
5. Give me an example or two of a good online privacy choice. [What about a bad privacy choice?][What do you think happens when someone makes a bad online privacy choice?]
6. I see you defined online security as [*response from questionnaire Q9*]. Do you think online security is important? [Why or why not?]
7. Give me an example or two of a good online security choice. [What about a bad security choice?][What do you think happens when someone makes a bad online security choice?]
8. I see you defined an online risk as [*response from questionnaire Q13*]. What are some examples of risky online behavior? Why do you think people take online risks? What happens to people who do [*repeat answers child just gave about online risks*]? Why do you think people make risky choices even if they know they're risky?
9. Can you remember making any risky choices online you can tell me about? Did you know they were risky at the time? What happened because of those risky choices?
10. What are the most important things you can do to stay private and secure online?
11. Who do you think is most responsible for keeping you private and secure online?

Pre-interview Questionnaire – Parents

1. What is your relationship to your child? [radio buttons: *Mom/Dad/Other relative or non-family guardian (describe)*]
2. What is your gender? [radio buttons: *Male/Female*]
3. What is your age? [entry field] (in years)
4. What is your highest level of education? [radio buttons: *Some high school/High school diploma/Some college/bachelor's degree/Master's degree/Doctoral degree/Other (specify)*]
5. What is your occupation? [text area]
6. How many children under 18 live in your household? [text area]
7. How many people in total live in your household? [text area]
8. In general, when does your household adopt new technologies? [radio buttons: *We try the latest technologies as soon as they come out/We follow technology trends/We let others work out the kinks first/We wait until our old technology dies/We wait until new technology becomes affordable for us*]
9. Do you own a smartphone? [radio buttons: *Yes/No*]
10. Does your child have their own or share a smartphone? [radio buttons: *Yes, their own/Yes, they share one/No*]
    [If the answer to Q10 is "No," then skip to Q11]
    10.1 At what age did you first give your child access to a smartphone? [entry field] (in years)
    10.2 On average, how many hours a day do you believe your child spends on a smartphone? [entry field] (in hours)
11. Does your child have access to computer(s) in your home? [radio buttons: *Yes, they have their own device/Yes, they share one with me or other family members/No*]
    [If the answer to Q11 is "No," then skip to Q12]
    11.1 At what age did you first give your child access to computers at home? [entry field] (in years)
12. How would you define online privacy? [text area]
13. How much would you say you know about online privacy? [radio buttons: *Very little to nothing/A moderate amount/A lot*]
14. How would you define online security? [text area]
15. How much do you know about online security? [radio buttons: *Very little to nothing/A moderate amount/A lot*]
16. Do you think your child always use electronic device(s) securely? (smartphone, desktop, laptop, tablet) [radio buttons: *Yes/No/I'm not sure*]
17. How would you define risky online behavior? [text area]

18. Have your spoken to your child about risky online behaviors? [radio buttons: *Yes/No/I don't remember*]
19. Do you think your child has been a victim of risky online behaviors? [radio buttons: *Yes/No/I'm not sure*]
20. Do you think your child has knowingly engaged in risky or negative online behaviors? [radio buttons: *Yes/No/I'm not sure*]
21. Do you think your child has more, less, or about the same, knowledge of technology as you? [radio buttons: *More/About the same/Less/I'm not sure*]

Semi-Structured Interview Scrip – Parents

1. Tell me about how you spend most of your time online. Do you think you and your child do similar things online?
2. Do you or does someone else monitor and/or limit your child's cell phone use? [If so, who and how? Why?]
3. I see you defined online privacy as [*response from questionnaire Q12*]. How, if at all, do you think online privacy matters in your child's life?
4. Describe good and bad online privacy choice. What are some of the consequences when children your child's age make bad online privacy choices? Have you talked with your child about these choices and these potential consequences?
5. I see you defined online security as [*response from questionnaire Q14*]. How, if at all, do you think online security matters in your child's life?
6. Describe good and bad online security choice. What are some of the consequences when children your child's age make bad online security choices? Have you talked with your child about these choices and these potential consequences?
7. I see you defined an online risk as [*response from questionnaire Q17*]. What sorts of risky choices do you think children your child's age make online? Why do you think children take online risks?
8. What are the most important things you think a child can do to stay private and secure online? What challenges, if any, do you face in helping maintain your child's privacy and security online?
9. Who do you think is most responsible for keeping your child private and secure online?

Appendix C

Example of coding process from first cycle codes through final theming of data

Research Question	First Cycle Sorting Codes	First Cycle Comparison/Discussion Codes	Themed Data
RQ3: How, if at all, do parents influence children's OPS understandings?	• P1a: Describes privacy (including extensions and descriptions from interviewee prior to the question 'do you think online privacy is important?') • P1b: Y1b: Privacy understandings (own or related to child) • Y1a: Describes privacy (including extensions and descriptions from interviewee prior to the question 'do you think online privacy is important?') • Y1b: Privacy understandings (including examples and explanations from interviewee prior to the question 'do you think online privacy is important?) • P2a: Describes online security (including extensions of defi • P2b: Online security understanding (own or related to child; include answers to "how do you know they're secure") • Y2a: Describes online security (including extensions and descriptions from the interviewee prior to the question' do you think online privacy is important?') • Y2b: Online security understanding (including examples and explanations) • P1c: Perception of the role/importance of online privacy to child • P2c: Perception of the role/importance of online security to child • P4d: Reports discussion privacy/security with children as a way to teach/regulate use (include stories) • P4e: Reports physically controlling/monitoring children' devices in some way • P4m: Does not monitor device use/activities	Abbreviated Codes: • Shared knowledge • Fatalistic • Agency/agentive • Believe in privacy • Conflicting beliefs • Consequences • Specific conversations • General "conversations" • Reactive conversation • Consequence-based conversations • Physical control • Device/technology monitoring • Privacy/security connection • Passive monitor • Screen time • Incident-based beliefs • Good kid syndrome • "Open door policy" • Cancel culture • Stranger danger • Deception-as-strategy	Steps: • Compare P1a & P1b with Y1a & Y1b at the dyad level and then cross dyad/grade level • Compare P2a & P2b with Y2a & Y2b at the dyad level and then cross dyad/grade level • Compare P1c & P2c with P4d, P4e, & P4m at the dyad and then cross dyad/grade level; then compare these results with Y1a, Y1b, Y2a & Y2b Results: • Parents who don't find P/S important don't talk about it • Parents of young children rely on parental controls, but don't love them • All monitoring decreases as youth age (within and cross case) • Most parents physically monitor AND have conversations • School is a trusted source • Conversations are reactionary and consequence-centric • Conversations are developmentally-perceived by parents • Higher knowledge = parents who have more conversations (younger) • More specific conversations = higher knowledge (younger)