A Comparative Study in the Effectiveness of Interactive E-books to Teach Children Online Privacy and Security

by

My-Linh T. Rouil

January 2021

Presented to the

Division of Science, Information Arts, and Technologies

University of Baltimore

In Partial Fulfillment

of the Requirements for the Degree of

Master of Science

Approved by: DocuSigned by: Kathryn Summers 2/1/2021
A10D371CA4EC43F...

[Kathryn Summers, Thesis Advisor]

DocuSigned by: 2/1/2021
E147E72B25744E6...

[Greg Walsh, Committee Member]

Abstract

The purpose of this study was to evaluate whether interactive e-books could as effectively teach online privacy and security to children ages 7 through 10 in Maryland, Virginia, and Maine as to Canadian children. The research replicated a study performed in Canada (Zhang-Kennedy & Chiasson, 2016), to see if the effects are the same. The study also investigated the persistence of the privacy models held by Canadian children identified prior to the COVID-19 pandemic, which had informed the design of the interactive e-book, amongst children in the Eastern Coast region of the United States. Fifteen parent and children pairs completed the study, which included a device criteria questionnaire, usability evaluations, a pre-privacy knowledge assessment before co-reading session, and a post-privacy knowledge assessment after a ten-minute distractor. Data analysis was conducted for all 15 parent-child pairs. During initial synthesis it became evident that the design of the interactive e-book was not suitable for children aged 10, which confirmed the intention of the original Canadian researcher to target young children aged 7 through 9. Therefore, results for two child participants aged 10 were excluded for the analysis that evaluated the e-book's effectiveness, but their results were included in the analysis for the persistence of privacy models. Children in the study showed an increase in comprehension of online security and improvement on safety-conscious behavior similar to the study involving Canadian children. However, children in the United States had less positive experiences with the interactive e-book than children in the Canadian study. Three mental models of privacy were found to have persisted amongst the child participants in the United States: 'to be alone', 'to hide

secrets/special things', 'to keep things to yourself'. One model did not persist after reading the e-book: 'to not talk to strangers' but evolved to 'don't *trust* strangers'. One new model was identified, 'don't let anyone see you'. Additionally, the study identified some of the ways that children's mental models of the world were impacted by the COVID-19 pandemic. Ultimately, the goal is to provide further empirical evidence and insight to inform the design of better cybersecurity tools for young children.

Acknowledgments

I would like to thank my thesis advisor Kathryn Summers for her encouragement to pursue research that was close to my heart despite the challenges of researching with vulnerable population; and for her guidance in shaping the direction of this thesis. I would also like to thank Greg Walsh, from whom I learned how to conduct research with children, and who introduced me to the master's program in Interaction Design and Information Architecture at the University of Baltimore. I have learned so much from both of you during my time here. In my first year of graduate study, I had a conversation with Greg where we discussed what design means. I defined design as a balanced composition, having had a career as a visual designer. I remember Greg countered with "design is problem solving" – that has now become my definition.

I would also like to thank my husband, Richard, who turned out to be my unofficial internal reviewer for this thesis, and the voice of reason whenever "mommy had a 'mom-nado'" trying to complete this thesis. I would not have come this far without your love, support, and believe in me. Lastly, I want to thank my daughter, Emilie, for inspiring this work; and my son, Alexandre, for all those nights he put himself to bed while I had to work on my thesis.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

Motivation

"I have a concern. Will the kids be playing games all night unsupervised or will you take their electronics away? There are safety risks they don't yet understand." - Sadie Hendrickson

This study was motivated by my concerns as a parent when my nine-year-old daughter discovered the world of virtual gaming and requested a "Roblox" sleepover birthday party. I found myself, along with other parents, trying to navigate how to keep our kids safe in their new digital playground. In my attempt to learn how to educate my daughter in this new space, I searched the internet for educational tools and literature on the topic of children and online security that could help her understand the potential threats of the internet. I found there was a lack of online privacy related educational tools that could effectively teach young children how to navigate digital spaces safely in a manner that they can relate and understand.

Although there are many privacy educational tools, few are geared towards young children aged 7-9, and often they are dense and text heavy, targeting an older audience. Since for most people security is seen as a secondary goal and the tradeoff of time for security is deemed as not worth the investment (Wash & Rader, 2011; Whitten & Tyger, 1999), these factors often deter even adults from investing time on learning security, not to mention children. However, with the unprecedented rise in children's screen time due to the COVID pandemic (UNICEF, 2020), the need for effective cybersecurity education tools to teach children how to safely navigate digital spaces has become even more dire. Notably, a study performed in Canada by Zhang-Kennedy & Chiasson (2016), *"Teaching with an Interactive E-book to Improve Children's Online Privacy Knowledge"*, and later

extended in 2017, *"Cyberheroes: The design and evaluation of an interactive e-book to educate children about online privacy,"* by the same authors, effectively showed improvement in children's online security knowledge and behavior in responding to online risks through privacy lessons presented in an interactive e-book using a superhero narrative. These two studies differed in study design and sample size. The 2016 study was a within-subject design with seven parent-child participants, focused on refining the educational e-book. The extended study was a between-subject quantitative study with a larger sample size of 22 parent-child participants, where the independent variable was the type of media (printed text vs. E-book) and the dependent variable was privacy proficiency.

Purpose and Contribution

I believe it is worthwhile to repeat Zhang-Kennedy & Chiasson's 2016 study to determine if a group of children in the United States can also benefit from improved online privacy knowledge and be better equipped to make positive security decisions. My study will replicate the original 2016 study, as enriched by data from the 2017 study, since the sample size was considerably larger. Replicating this study will allow us to compare the effectiveness of the interactive e-book in increasing the children's understanding of online safety and privacy.

The goal of the research is to provide more evidence-based findings for the effectiveness of interactive e-books as a tool to help young children in the United States learn online security so that they can be responsible digital citizens. The contributions of my study are: (1) the results of both quantitative and qualitative comparative analysis

between children of different geographical and cultural groups on the effectiveness of using an interactive e-book to teach children's online privacy, and (2) to provide perhaps the first study to investigate the persistence of children's mental models of online privacy after the intervention of an interactive e-book in the Eastern Coast region and within a pandemic time. The results of this study can then be used to inform the design of cybersecurity learning tools for young children aged seven to ten.

Research Question and Scoop

The study is guided by the following research questions:

1. Can an interactive e-book be as effective in teaching online security to young children (aged 7 through 10) in the United States as it was in the study performed on Canadian children? If so, how do the results from both studies compare in improving children's online security knowledge and privacy-decision-making behavior?
2. Did the current mental models of children's conceptualization of online privacy change or persist over time, culture, and location? Did the intervention of the interactive e-book change children's model of online privacy?

I conducted a within-subject user study of 15 parent-child pairs with children participants aged 7 through 10 in the United States. Most participants were drawn from Maryland and Virginia. The study included: pre-evaluation and post-evaluation for parents and children, usability evaluation, a distraction session, questionnaires, and interviews. Between pre-evaluation and post-evaluation, parent-child pairs co-read the

interactive e-book (“Cyberheroes”). Children engaged in a 10-minute distraction activity after the usability evaluation, while parents completed their usability evaluation. Results from both quantitative and qualitative data were coded for analysis and compared against the original study. Findings and implications on children’s online security knowledge will be discussed.

Chapter 2: Literature Review

Introduction

Mobile media has become a universal part of children's media landscape across all levels of society ("The Common Sense: Media Use by Kids Age Zero to Eight," 2017). In the new era of the coronavirus (COVID-19) pandemic, the rise in children's connectivity has been unprecedent. More than ever before, millions of children are exposed to on-line privacy risks as schools and social interactions are overwhelmingly confined to children's screens (UNICEF, 2020). Young children are the most vulnerable to online threats, due to their lack of maturity, knowledge, and capacity for judgment to safely navigate online spaces (Zhang-Kennedy et al., 2017). Despite this fact, there is a dearth in the literature on young children and cybersecurity. Most literature on children and cybersecurity are focused on tweens and teenagers (Zhang-Kennedy et al., 2017). The same holds true for cybersecurity educational initiatives, with many initiatives focused on tweens, teens, and adults as their primary audience (Sharples et al., 2009; Steeves, 2014). Amongst the few educational resources that purport to be designed for children, it is unclear if any of them were actually *with* children, nor has their effectiveness in boosting children's security knowledge been evaluated (Kumar et al., 2018). There is an irrefutable need for age-sensitive educational tools to empower young children to be secure-digital citizens.

In light of the recent COVID-19 pandemic that has shocked the world, the issues of online safety and how to effectively educate the most vulnerable to make security conscious decisions is even more pressing. It is well recognized in the literature that

usable security decisions are based on their users' mental models describing how someone thinks about a problem (L J Camp, 2009; Wash & Rader, 2011). Therefore, to effectively teach online privacy and positively influence security decisions requires an understanding of children's mental models of security and threats. It is also likely that the pandemic has influenced children's mental model of threats in their new reality. As such, this study leans on prior works by Leah Zhang-Kennedy et al. (2016) from her first study on children's perception of mobile threats, *"From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats,"* and her second study (Zhang-Kennedy & Chiasson, 2016) on improving children's online privacy knowledge with an interactive e-book, *"Teaching with an Interactive E-book to Improve Children's Online Privacy Knowledge".* However, attention during coding of the results was also paid to mentions of the pandemic, to see if the pandemic had a discernible influence on children's mental models relating to security and online privacy.

Zhang-Kennedy, et al. (2016), first identified gaps in children's online privacy conceptions. This study found that children' conception of online privacy is based on their understanding of physical privacy and safety, and five mental models of children's perceived mobile threats were identified. Zhang-Kennedy & Chiasson (2016) used these findings to inform the design of the interactive e-book. This study employed physical privacy concepts as metaphors to communicate online risks that the authors considered relevant to children. These risks included: 'disclosure of personal information', 'passwords security', 'geolocation sharing', 'cyberbullying', 'online trust', and 'online tracking' referred to by the authors as 'digital trails'. Both studies were performed on

Canadian children. While the second study reported considerable privacy knowledge improvement after interaction with the e-book, the study sample was not geographically diverse.

The overarching goal of this thesis is to contribute to better designed cyber security tools to help young children be safer online. To this end, my thesis replicates the work of the authors Zhang-Kennedy & Chiasson (2016) to evaluate the effectiveness of the interactive e-book as a teaching tool for improving online privacy knowledge with children aged 7 through 10 in the United States (research question 1). Subsequently, the study compares the mental models of my research participants to the mental models identified by Zhang-Kennedy et al., and further explores whether these mental models were affected by interaction with the e-book (research question 2). Finally, my study identified and described impacts from the COVID-19 pandemic on the participants' discussion of their online experiences.

The purpose of this literature review is to gain insight to the factors that should be considered to design effective cybersecurity educational tools for young children. In this review, I give background on the state of online connectivity amongst young children and the risk that arises with their increased online exposure. I focus on the increasingly urgent online risks young children face in their new reality compared to the risks children faced prior to the pandemic as reported in the Canadian study. I give an overview of the challenges of designing cybersecurity education for children. I focus on current understanding of children's mental models of online privacy, and I discuss the role mental models play in improving children's cybersecurity knowledge. Lastly, I give an

overview of the learning effects of interactive e-books and discuss design guidelines for children's interactive e-books.

While I give background on children's mental models of the source and types of online threats models, this study focuses on children's mental models of what it means to be safe and private, and on the potential use of interactive e-books as a viable learning tool to improve their knowledge of online privacy.

State of Children's Online Connectivity

According to a nationwide media use survey by Common Sense Media's (2017) young children aged 8 and under in the United States have become universally exposed to mobile media across all levels of society, with nearly 93 % of children accessing mobile devices as early as infancy. Since 2011, media consumption in the U.S. has tripled every three years amongst young children, leading to an average of two hours daily in 2017, with 72 % accessing mobile devices regularly. Nearly all (98 %) children age 8 and under in the U.S. now live in a home with some type of mobile device, regardless of social or economic levels. From birth to the age 8, the study reported that children in the U.S. are engaged in various forms of digital content, with their primary activity being watching video from YouTube and with video gaming as the second preferred activity. The study did not include children's screen time for school.

In 2019, Common Sense Media (Rideout & Robb, 2019) expanded the survey to tweens (aged 8 through 12) and reported their daily online screen time was approximately five hours. This study also did not include screen time for school.

Additionally, the study reported similar findings for tweens in terms of their most popular online activity as watching YouTube videos, with 56 % viewing at an average of an hour per day. In fact, online video viewing through mobile devices was described as "through the roof" with more than twice as many tweens viewing online videos, and the average time had doubled since 2015. In addition, the study's showed that although YouTube specifies a requirement of at least 13 years for its viewers (http://youtube.com), 76 % of children aged 8 through 12 watched YouTube instead of YouTube Kids, with 67 % of children reporting "a lot" of enjoyment (Rideout & Robb, 2019). In fact, only 7 % of children watch YouTube Kids as compared to 53 % reporting YouTube as "the most" watched. This indicated a clear vulnerability in the platform's success (and perhaps its commitment) to screening for underage users, which poses a risk that children may end up viewing inappropriate content.

Neither the 2017 nor the 2019 Common Sense' survey addressed why young children gravitated towards online content that was not geared for their age group nor did it report why children were able to access such content. It can be reasoned that since young children used mobile media primarily for entertainment (Livingstone, 2006; Zhang-Kennedy et al., 2016), the wider selection of content on the mainstream YouTube channel offered more entertainment variety. It is also plausible that appropriate security restrictions might not have been put in place by parents to limit children's content access. Both studies consistently projected that the rate of mobile media consumption tripled every three years, with the 2019 survey pointing out that increased usage comes with increased risk of exposure to inappropriate content. Moreover, children are currently

faced with even greater exposure to online threats, since the disruption of the COVID-19 pandemic caused many schools to switch to remote learning and limited children's social interaction to online (UNICEF, 2020).

Thus, the COVID-19 pandemic plays a historic role in the unparalleled level of connectivity amongst an entire generation of young children, with accompanying safety risks, on top of the near saturation of online access in the United States prior to the pandemic. Most early studies on young children's online activity during COVID have focused on children's mental health, but scholarly studies specifically investigating elementary age children's online privacy and security risks in the context of COVID need to be performed. Anecdotal evidence indicates that these risks have skyrocketed, with media reports of Zoom bombing, etc. Thus, studies such as this thesis research have become even more urgent.

Children's Online Risks

As screen time rises for millions of children, parental concerns heighten for their safety and security as children's exposure to potential online risk increases. Common risks that children can face online include exposure to inappropriate content (sexual or violent), dangerous personal interaction (cyber-bullying, sexual predation) and economic/technical dangers (exploitative data mining, phishing, scams, even malware) (Kumar et al., 2017; UNICEF, 2020; Zhang-Kennedy et al., 2016). Prior work has identified that the main risks to children and adolescents' privacy and security online stem from their improper use of technology, lack of understanding of privacy issues (including inappropriate disclosure of personal information, whether by posting

information on social media that may compromises their privacy or by providing personal information in chats), and finally an inability to recognize false actors (O'Keeffe et al., 2011). Ironically, children can also face risks from poor-quality surveillance by often well-intended parents who supervise their children online activities, but who do not exercise best practices in security management or privacy behavior themselves. Examples include using auto-check passwords, handwriting passwords down, encouraging children to use easy to remember passwords, or posting their children's photos and personal information on social media sites (Livingstone, 2006; Livingstone et al., 2012; Zhang-Kennedy et al., 2016; Kumar et al., 2017). For young children (age 7 through 11), many parents are particularly concerned about the physical and mental safety risks from exposure to inappropriate content, or from encounters with external threats from potential predators (Kumar et al 2017; Zhang-Kennedy et al., 2016).

Hasebrink, U., Livingstone, S., Haddon, & L. Ólafsson (2009), in a comparative study investigating opportunities and online risks amongst European children, identified three classifications of online risk to children: (1) content, (2) contact, and (3) conduct. The risk of content refers to children's exposure to inappropriate online content such as explicit imagery, extremist content, or misinformation; the risk of contact refers to being contacted by predators or users with ulterior motives, including tracking of personal information through data mining of digital records; and the risk of conduct has to do with children themselves acting inappropriately or aggressively online.

Nearly all of these risks have been heightened by COVID-19. Research on sexual predators claims predators engage in a "seduction stage" known as "grooming" prior to

the abuse (Bennett & O'Donohue, 2014). The molesters build a trusted relationship with the child, and then manipulate them to be compliant to abuse such as sending inappropriate photos or video. Perpetrators may lure the child to meet in person. The offender subsequently uses these acts performed by the child as blackmail or makes threats to continue the abuse. The National Center for Missing and Exploited Children (NCMEC) reported that within the month of March 2019 there was a recorded 106 % increase in reports of suspected online child sexual exploitation (Brewster, 2020). In addition, based on INTERPOL Assessment Report (2020) "there is an under-reporting of child sexual abuse and increased sharing of child exploitation content through peer-to-peer networks ...amongst the effects of the COVID-19 pandemic". The worldwide increase in grooming behaviors due to the increased time children spend online for school, entertainment, and social purposes is made even worse by the accompanying limited access to community support services through school personnel, who traditionally play key role in reporting cases of abuse, has led to an under-reporting of child sexual exploitation.

Cyberbullying has also increased by 70 % during the COVID pandemic. The rise in cyberbullying is associated with pandemic stressors that cause kids to lash out (Gordon, 2020). Cyberbullying is the intentional use of digital media to communicate false, embarrassing, or hostile information about another person, and can have tragic psychosocial outcomes such as depression, anxiety, and suicide (O'Keeffe et al., 2011). Cyberbullying can include hacking into children's account or stealing online identity to humiliate the child (Kaspersky, 2020). Cyberbullying can also include being left out of an

online group, which increases children's sense of isolation, and anxiety. Prior to the pandemic, research consistently reported that teenagers were more vulnerable to online harassment, including cyberbullying and sexual solicitations, than younger children (aged 11 and under) due to findings that younger children are predominantly not involved with social media content and do not spend as much time online as teenager (Kumar et al., 2017; Livingstone et al., 2012; Wisniewski et al., 2017; Zhang-Kennedy et al., 2016), but statistics have shown that this has pervasively changed with COVID.

The risk that children will encounter age-inappropriate or harmful content has increased as well. Partly this increased risk results from the increased time spent online, but it has also been a result of deliberate "Zoom-bombing," where malicious actors hijack a Zoom meeting (often used for school meetings) to display offensive material. The FBI has received hundreds of reports of Zoom-bombing with image of child sexual abuse. Moreover, children now are more likely to come across content that could incite suicide, self-harm, violent, or radicalization of political, religious, or racist views escalated by mounted pandemic tensions, and children may face an increase in suicide rates due to increased mental health issues (Buck, 2020).

A final risk to children's privacy that has been amplified by the pandemic is the collection of personal information. According to the Children's Online Privacy Protection Act (COPPA), information operators of websites and online services in the U.S. are prohibited from collecting personal information on children under 13 (Federal Trade Commission, 1998). Unfortunately, since COPPA does not require operators to ask children's age, many mobile apps fail to abide by the provision (Federal Trade

Commission, 1998; Kumar et al., 2018). The apps that collect illegal information about children include apps children use for remote school. Hence children's privacy, and personal data, including associated digital footprints of children's online activities, preferences, and location, are at risk of being collected, compromised, shared online, and exploited. In addition to the Zoom bombing mentioned above, cybercriminals have compromised hundreds of Zoom accounts and posted personal identifying information (PII) on the dark web (Christine R, 2020; Jamie, 2020). These incidents of privacy and personal information being threatened and compromised are a risk with any app that does not abide by the provisions for child protection set out by COPPA.

In conclusion, the literature shows that much of the online risks children face in the reality of COVID-19 existed before the pandemic, but these risks have now become even more acute. Some of these issues need to be addressed by vendors, by legislation, and by parents. But some of these risks can be reduced by helping children improve their mental models around security and online privacy. A subsequent section will address these mental models.

Parental Concerns with Children's Online Privacy Risks

As online connectivity becomes a universal part of the children's landscape, parental concerns rise over children's online safety. COPPA stresses that parents are primarily responsible for supervising their children's on-line activities, deeming parents to be accountable for information collected on their children. Prior research on parents' protective strategies to regulate children's online activities found that young children

have few protective strategies of their own, and largely rely on their parents (Kumar et al., 2017; Zhang-Kennedy et al., 2016).

Zhang-Kennedy et al. (2016)'s investigation on children's online privacy and parental surveillance confirmed that parents do feel a strong need to protect young children from online threats. According to the authors, parents' concerns around children safely navigating online spaces are "due to young children's level of maturity, inexperience, and knowledge". Furthermore, the study found that while parents do want to teach young children about online risks, they also want to "shelter them from online negativity, such as inappropriate content geared towards teens or teenagers". Parents were also cautious about early exposure to social media. As such, many parents employed protective strategies to regulate children's internet use, such as device monitoring, setting rules for device use, limiting contacts to families and close friends, and using apps that have pre-selected text messages.

What Children Need to Know About Cybersecurity

Parents have always played a major role supervising their children's online activities to protect them from harm, but as mobile media become pervasive and more households are connected to multiple devices, it becomes increasing difficult to manage and supervise children's online activities ("The Common Sense: Media use by kids Age zero to eight," 2017). Additionally, the pandemic has further strained parents' time as parents have to manage work life while homeschooling their children, which reduces their availability to manage an already complex responsibility of regulating children's online activities. While education is a form of mitigating children's online risks, few

children have training or formal education on security and online privacy (Kumar et al., 2018; Livingstone & Bober, 2004).

It is true that some of children's online risks stem from their misuse of technology and flawed understanding of online privacy issues, leading to actions that compromise their safety. The good news is that children are capable of complex learning (Kumar et al., 2018; Perner, 1983) and their behavior can be positively changed through effective education (Zhang-Kennedy et al., 2017; Zhang-Kennedy & Chiasson, 2016). It is of value to the world and a humanitarian responsibility to teach children how to safety learn, play, and socialize online so that they may grow into healthy, responsible digital citizens.

The three categories of risks identified by Hasebrink, U., Livingstone, S., Haddon, & L. Ólafsson (2009) provide a useful framework for setting educational goals around security and online privacy. These categories are content, contact, and conduct. We can help children curtail their risks online by teaching them the following:

(1) **Content**: to recognize inappropriate content as content that could make them feel uncomfortable, confused, upset, scared or hurt, and to tell a trusted adult immediately

(2) Contact: to not trust someone online whose real identity is unknown to their parents

(3) **Contact**: to recognize unsafe and unwanted online advances such as sexting, sending explicit imagery, luring to meet in person, attempts at isolation, and to tell a trusted adult of such encounters

(4) **Conduct**: to not engage in bullying by responding to threatening email, messages, text, or post and to tell a trusted adult of such attempts

(5) **Conduct**: to not reveal private and personal information inappropriately (name, age, password, address, location sharing, school, or personal identifying information); and to not post or trade personal photos that could compromise their safety.

While teaching children 'what to do' is a step forward, it is of more lasting value to teach children 'why' such actions are necessary, and such instruction will result in better outcomes of privacy and safety online (Zhang-Kennedy et al., 2016; Halford, 2014; Camp, 2009). In other words, teaching children critical thinking about the consequences of their decisions will empower them to make positive security decisions so they can more safely navigate the evolving landscape of online security risks.

Cybersecurity Education Challenges

The primary challenge with educating end-users to improve their online security decisions is that most users (adults and children) regard security as a secondary task that is at odds with their primary task (Whitten & Tyger, 1999). There is a tradeoff that exists between users investing time to enact proper security protocols versus achieving users' primary goal. Additionally, security information is often dense and considered technically complicated, leading to user frustration and abandonment of proper security efforts (Herley, 2009; Wash & Rader, 2011; Whitten & Tyger, 1999). Most security information tells users what they should or should not do, but does not give adequate explanation to

communicate the value of their invested time enacting the security precautions that would result in better security outcomes (Zhang-Kennedy, 2013).

The challenge to convince children to behave in a privacy-preserving manner is even more difficult for several reasons. First, young children are emerging readers and security information often is communicated through complex, technical language. Second, as with adults, security is not a primary goal for children. In fact, children's primary goal for engaging in online activities is generally entertainment (Zhang-Kennedy et al., 2016, 2017), whereas adults are more likely to have specific goals and tasks they wish to accomplish. This focus on entertainment positions children to be even less cognizant of anything else beyond the criteria of entertainment and fun. Third, there are many factors that affect privacy and security such as culture, age, and social-economic status, which make defining the concepts of security and privacy difficult for the general public (Livingstone, 2006) much less children who lack experience, knowledge, and the capacity for self-regulation. Fourth, information security choices provide little direct feedback unlike physical security (Wash & Rader, 2011). For example, the smoke alarm will immediately beep when it detects smoke, but users may not find that they were involved in credit card theft until well after the incident, and they may not be able to link the security breach with a specific decision or action.

Lastly, research has found that even adult users have poor mental models of security threats, which frequently lead to negative consequences based on their behaviors (Wash, 2010; Zhang-Kennedy et al., 2016). Early research has shown that children's mental models of privacy and security are even more flawed, differing from those of

adults due to children's lack of autonomy in many aspects of their lives, and developmental capacity. As such, research argues that cyber security education tools should teach children critical thinking about the consequence of their online actions (Steeves, 2014), and improve mental models (Zhang-Kennedy et al., 2016), in order to influence behavior (Sharples et al., 2009; Camp 2009).

My research focuses on the last education hurdle pertaining to young users' mental model of online privacy, trying to use narrative and interactivity to help children improve their mental models through effective cybersecurity education for young children.

Mental Models and Decision Making

The relationship between mental models and decision-making was first identified in 1943, by Kenneth Craik. According to Craik, the mind constructs "small-scale models" of how something works in reality (Gregory, 1983). People rely on these models to solve problems, acquire new knowledge, and anticipate the outcomes of various actions. His findings were later echoed by Johnson-Laird (1985) who hypothesized that thought models are parallel realities by which humans "try out various alternatives" in order to choose among possible actions. The mind uses prior knowledge of similar problems to predict cause and effects (Johnson-Laird et al., 1998). In essence, mental models help humans understand and respond to the world by shaping the connections and opportunities we see in it. They are behind decision making and shape our behavior.

Measurement of children's understanding of security and online privacy must measure authentic comprehension rather than successfully executed applied rules.

Halford (2014) agrees that the most important questions in child learning are how children acquire information, how they represent it, and how they used these presentations to build problem-solving strategies. By first identifying a child's mental model about security and online privacy, we can leverage more robust insights into children's mental model of related concepts. This creates the opportunity to better promote children's understanding of concepts by using their mental model where suitable to explain new concepts with meaningful similarities or improve on these models if they were founded on misconceptions. The latter premise is a focus of this thesis as it pertains to the second research question this study aims to answers: have children's current mental model of online privacy and security changed or persisted over time and culture, and do these mental models change as a result of an educational intervention with an e-book?

Mental Models of Online Privacy and Security

Prior work in usable security with adults has attempted to understand user's mental models in order to influence decision making. Jean Camp (2009) argued that an accurate mental model could significantly improve risk communication by using metaphors and analogies to explain complex security risks. According to the author, to influence good security behavior requires communicating risks in a way that users can imagine the error or consequence associated with the risk in order to adequately evaluate their decisions. The author illustrates the effectiveness of this method in an example of password security: the admonition to "create passwords that are hard to remember, do not reuse passwords" is not an easy to imagine response. Conversely, "passwords are like

toothbrushes; they should never be shared" is an easy to imagine response, communicating a clear requirement for secured passwords.

Camp (2009) identified five mental models using metaphors and analogies to communicate common computer security risks to the general public: physical security, medical infections, criminal behavior, warfare, and economic failure. Physical security is intrinsic in physical objects and is invoked with metaphors such as "locks" and "keys" indicating individual and localized control. The medical infections model is analogous to the spread of infectious diseases by the diffusion of malicious code (viruses). This use of public health metaphors helps to illustrate a complex concept of malware risk in networked security, such as the infected person may be asymptomatic, but they could still propagate the spread of the virus to other potentially vulnerable users. Criminal behavior models link computer security to larger crimes where either the individual or system are target of attacks. By linking computer security breach to criminal activities, it is easier for users to imagine themselves as victims and alter their behavior to prevent risks. The warfare model implies the presence of an advancing enemy and uses metaphors such as firewalls as lines of defense. Lastly, the economic failure model is analogous to the market where network and security vulnerabilities can result in economic losses associated with downtime. These five mental models of computer privacy and security risks have been used to effectively influence behavior by communicating cybersecurity vulnerabilities to the general public in a manner that enables users to visualize associated risks, with the associated power to influence behavioral change (Wash & Rader, 2011).

Children's Conceptualization of Online Privacy

Children perceive and experience the world differently than adults. As such their mental models of online privacy and security risks also differ. Therefore, it is necessary to understand how children perceive their own privacy and security. More research is needed into elementary school-aged children's mental model of online privacy and security (Kumar et al., 2017). Children's ability to understand the concept of deception and secrecy (Colwell et al., 2016) is dependent on their early (ages 4-6) development of a "theory of mind" – the capacity to understand that people have different mental states from their own (Pavarini et al., 2013), and an understanding that people's actions are guided or misguided by the truthfulness or falsehood of their beliefs (Perner, 1983). Children's understanding of the concept of deception and secrecy are the basis for safeguarding privacy, personal information, and anticipating malicious intent from others.

Amongst the few studies identifying young children's mental models of online privacy and security are work by Zhang-Kennedy et al. (2016), which was later extended by Kumar et al. (2017). Zhang-Kennedy et al. (2016), *"From Nosy Little Brother to Stranger Danger,"* interviewed 14 parents and child age 7-11 in Canada to explore perception of mobile device-based threats by children and parents. The work used Grounded Theory to identify four mental models of privacy held by children: (1) to be alone, (2) to hide secrets or special things, (3) to keep things to yourself, and (4) to not talk to strangers. The study also identified four child threat models held by children: (1) from peers, (2) from 'bad' media, (3) from 'mean' strangers, and (4) from parents.

Children's Online Privacy Model

The study reported that more than a third of children ages 7-11 "showed a lack of understanding of what it meant to be private online", since their definition was based on physical privacy. Children in this group equated privacy with tactile objects such as locked doors when you want 'to be alone' (5 of 14 children) or 'to hide secrets or special things' (3 of 14 children). Conversely, children who defined privacy as 'to keep things to themselves' (4 of 14 children, all ages 9-11) and 'to not talk to strangers' (2 of 14 children) did have a basic understanding of the online privacy as they framed it in the context of safety and safeguarding personal information.

The first model of privacy is 'to be alone' or 'to be by myself' was held by the largest group of children (5 out of 14 children). This group associated online privacy with privacy defined as rooms where children could control entrance with locks or confine themselves by closing the door or "really lock it [door]" if they wanted "to be alone" such as when they are taking a shower. The second model of privacy is "to hide secrets or special things"; these three children reported descriptions of hiding physical objects such as an iPad from a younger sibling to protect it from being broken or hiding a secret that you're not supposed to tell people, "like passwords". Few children were able to explain why passwords were secret, even though all children associated passwords with secrets. The third model of privacy is "to keep things to yourself," with four children reported as having this preliminary understanding of online privacy. To this group, privacy meant keeping personal information to yourself including: events, posts, and data. Children in this group were aware that people can "take" your personal data so it should be kept

private “only for yourself”. One expressed caution with posting information that “you might regret later”. In this study in 2016, nearly all the child participants (13 out of 14 children) were content consumers rather than content creators or contributors (Zhang-Kennedy et al., 2016). However, four years later, and ten months into the pandemic, many children in the United States are comfortable posting comments and chatting online. Lastly, the fourth mental model observed, “to not talk to strangers,” was the least reported with only two children in this category. Children framed these concerns in the context of safety: “it’s about keeping it safe”. Other reported descriptions in this category included not ‘lurking’ around people you don’t know and avoiding the risk of someone “being rude to you” online. Apart from the concern of a stranger being rude, the study did not report safety concerns associated with cyberbullying within any of the four privacy models. Nor did parents in the study report any incidents of an encounter with a stranger online or cyberbullying.

In summary, most young children’s mental models of online privacy were insufficient to motivate secure behaviors, although older children (age 9-11) showed a basic understanding. However, among those that showed basic understanding, it is unclear whether children’s statements reflected their own beliefs or if they were adhering to rules learned from parents; the study reported “they had a vague understanding of the reasons and seemed to be following the rules set out by the adults” (Zhang-Kennedy et al., 2016).

Children's Threat Model

The same authors also reported four children adversary threat models concerning children as potential threats from their peers, from media, from strangers, and from parents. Findings from the study reported that "children were mostly reactionary with "few protection strategies of their own" and tended to respond to threats by avoiding content with bad words or becoming "upset". Children's primary concerns with online dangers differed from their parents and revolved around more trivial security breaches, such as peers tampering with their games or misusing their passwords, while parents perceived external risks as a higher concern.

Nearly all the children in the study were concerned about threats from their peers (12 out of 14 children), with concerns ranging from siblings competing for shared devices, damaging their 'special things', or being bad at 'keeping secrets', while friends posed threats to participants internet access by sending inappropriate content such as a 'bad' word and getting child participants into trouble. Children's main concern with sharing game accounts with friends was that the friends could 'mess up' their game.

The second threat, from 'bad' media, came from inappropriate content that is violent, uses 'bad' words, or includes adult content (9 out of 12 children). Most children in this group were reported as not clearly understanding why certain content was considered inappropriate. For example, a child was confused as to why it was okay for him to play games with swords but not guns.

The third threat model from 'mean' strangers was reported as a concern by only five of the 14 children as an online threat, "even though most children agreed that you

should not talk to strangers offline". Additionally, most children assessed who was considered a stranger based on the person's friendliness online. Concerns were mainly around being teased by strangers with one child (age 8) who thought you should hide things from strangers that they can use to make fun of you such as not giving them your real name "so they could not make fun of your funny middle name". Another child (age 7) expressed concerned with bullying and considered that being safe online means not contacting people that "are not nice". The study reported only one child who perceived strangers as a threat associated with child exploitation, explaining that someone could seem friendly online but in reality, want to track him and physically harm him. The description reported in the study follows: "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".

Lastly, four of the 14 children perceived their parents as a threat, focusing on parents' invasion of their privacy as a potential risk by actions such as deleting apps on children's devices or restricting access to their devices. One child (age 9) reported deleting his browser's history to circumvent being monitored. Other studies have documented the ways in which parental surveillance can be perceived negatively by children, and have explored the rocky path to appropriately making space for developmental growth through allowing children increasing amounts of online privacy (Livingstone, 2006; Nolan et al., 2011; Steeves & Jones, 2010).

Overall, the study by Zhang-Kennedy, et al., (2016) suggested that children's reliance on off-line mental models of privacy affected their ability to anticipate online threats. Therefore, children had less concerns of safety risks online. External threats from

'stranger danger' online or being bullied was not perceived by most children as an impending threat, with only two children describing it as a concern. The study suggested that parents employ protective strategies to counterbalance children's lack of concern about 'stranger danger' including: prohibiting online chatting; using parent-controls; requiring permission to download an app; screening contacts on devices, restricting social media contacts to family and close friends, enabling privacy settings; and sometimes allowing only safe-texting app to select from predefined messages. Thereby, the "risk[s] from online predators, pedophiles, cyberbullies, cybercriminals, and other online dangers are less likely to occur for younger children due to their small online presence" (Zhang-Kennedy et al., 2016).

The contrast between children's primary safety concerns (internal threats such as parents and siblings looking at device or friends asking for a password, and parents' primary concerns with children viewing inappropriate media or with threats from strangers was stark. Ironically, internal risks to children's online safety were more common from parents and trusted adults who did not exercised good security practices themselves; many of the parents in the study posted children's photos online; encouraged easy to remember passwords; reused passwords; and wrote passwords down.

Cybersecurity Education Based on Children's Mental Models

Zhang-Kennedy and her colleagues used these four models of privacy to identify gaps in understanding to try to design an educational intervention that would leave children better equipped to make safe decisions online. For example, the belief that by closing or locking a physical door means you are 'left alone' is a fallacy as online

activities leaves records, i.e., digital footprints, which could be used in data mining to collect location, interests, preferences, and personal information.

In general, Zhang-Kennedy and her colleagues found that the limitations of children's mental models meant that children were unable to explain why particular safety and privacy behaviors were desirable. This echoes findings from Kumar et al. (2017), "that children ages 5-11 largely rely on explicit rules, rather than internalized norms, to determine when information can be disclosed online".

For example, children with the mental model of 'to hide secrets or special things' could articulate 'what they should not do' with passwords, but most could not explain 'why' it was important to not share passwords. Evidence of password risks were revealed in children's false belief that "no one wants to know what it is"; or that sharing passwords to trusted friends is acceptable. Therefore, children need to be taught that password sharing with friends poses the same risks as those with unknown individuals. One helpful approach is to use examples that make it easy to imagine the consequences associated with risks, and to be effective, these examples and analogies must be relevant to them (L J Camp, 2009; Wash & Rader, 2011; Zhang-Kennedy et al., 2017). For example, some children would be more motivated not to share passwords with friends if they understood that sharing passwords with your best friend is like giving them permission to take control of your games—a concern that is familiar to children.

Similarly, children with the third and fourth models of privacy identified by Zhang-Kennedy, et al., described as "to keep things to yourself"' and "to not talk to strangers" had only generalizations about what type of information should be kept private

such as, “things and events in your life”, “personal data”, or things that are “too personal”. One child tried to explain the need for privacy in a circular way: “people can take it [personal data] and you want to keep them private for only yourself”. Another child was wary of potential negative consequences of posting content, saying “do not post things that you don’t want to post…you may regret it later,” but it was unclear if these children were simply executing protective rules employed by their parents or whether they could discern which types of personal information are sensitive and under what conditions specific personal information would be acceptable or not acceptable to disclose.

Only two participants in Zhang-Kennedy's study said that they should “not talk to strangers.” For at least one participant, “strangers who were approved by parents were considered safe” even if the child may not have had any prior experience with the individual. Such was the case with a child disclosing her password to the researchers (Zhang-Kennedy et al., 2016). More concerningly, most children judged a stranger based on the how friendly they were online, which increased their vulnerability to grooming.

In order to help develop children’s understanding of information sensitivity in its varying context and form, children need fundamental lessons in online information flow and how contextual norms based on the situation and actors involved influences what type of information are sensitive. First, to help children understand what information can be disclosed online, children need to be taught the ecosystem of the web (i.e., the nature of information flow online) (Kumar et al., 2017). This will help them be aware of the point of visibility in their online activities as well as build the foundation for complex

concept of data mining. Second, children need to be taught that information sensitivity depends on the nature of the information (i.e., the type of information), the context (i.e., the situation pertaining to the information), the actor(s) involve in the information exchange, and the purpose (i.e., what is the need for the information, especially if it is not required). For example, a teacher asking for age in the context of administering a lesson makes what would typically be deemed as personal information not sensitive and appropriate to disclose. On the contrary, an unknown actor asking for age in a chat room when there is not a legitimate need, would make the personal information sensitive and therefore should not be shared.

These educational goals may seem unrealistic for children, since many adults also struggle to understand and follow good online safety practices. However, the literature suggests that role playing with children hypothetical situations can help foster critical thinking skills so that children build an awareness to the nuances of information sensitivity (Kumar et al., 2017).

Therefore, children need to be taught that they should not trust strangers online whose true identity is unknown, because people could pretend to be ‘friendly’ to gain their trust, but in reality want to cause them harm, such are the strategies of predators discussed previously. Additionally, children need to be taught how to recognize predatory behaviors and identify the warning signs that is associated with predators. By training children to “recognize and identify that repeated questions that are fishing for personal information when the information is not required are red flags, will help them better judge the sinister motives of the individuals” (Oglethorpe, 2020). Some of the types of

questions children should be trained to be wary of are those that ask for physical descriptions and make attempts to isolate the child to be alone with the individual. These questions may ask for: age, gender, address, type of clothes they're wearing, sending photos (nude, selfie), chatting privately or on another platform, whether parents monitor their devices, or meeting in person.

In conclusion, there is a disconnect between young children's understanding of privacy and safety online as revealed through their identified mental models of online privacy and threats. Therefore, educational tools should be designed to improve children's underdeveloped mental models of online privacy (Zhang-Kennedy et al., 2016) with the objective to teach critical-thinking skills that will influence positive security behavior online (L J Camp, 2009; Steeves, 2014). Based on the literature on mental model and usable security, this could be achieved in several ways. First, educators can leverage parallel concepts of privacy and safety that children have already experienced in the physical world to communicate safety and risks in the digital world (Zhang-Kennedy et al., 2016). Second, work from Camp (2009) showed evidence that communicating cybersecurity risks with simple metaphors and analogies that make it easy for users to imagine the consequences of their actions can effect behavioral change. Finally, the use of roleplaying and narratives to explore relevant situations and potential outcomes can help children develop more context-sensitive decision-making skills.

I propose that the medium of interactive e-books can be used to communicate online security risks to young children with metaphors that resonate with them, while simultaneously leveraging the use of imagery, narrative, differentiated instructions (i.e.,

tailored instructions to meet individual learning needs), and role-playing (Schugar et al., 2013). This approach can scaffold learning and help children solidify and internalize safe security and online privacy choices.

Teaching with Interactive E-Books

Rationale for Interactive E-Books

There are numerous reasons in the literature that argue for the potential of interactive e-book to have a positive effect on children's learning, which positions it as a viable tool for teaching. The most compelling is that e-books have the potential to alter the way content in text and pictorial form is read, consumed, and experienced due to their interactivity and convenience (Schugar et al., 2013). While traditional picture books have many of the characteristics found in e-books, including words, visual imagery (graphics, illustrations, photos) and narrative, they do not have the multimodal features of sounds, animations, videos, special effects, and adaptable narrations provided by interactive e-books (Schugar et al., 2013). When strategically implemented to support comprehension (Korat & Shamir, 2007), interactive e-books have the following benefits: (1) scaffold children's learning (C. Pearman & Chang Ching-wen, 2010); 2) enhance children's engagement (Druin & Solomon, 1996); and (3) support individualized instructions (Schugar et al., 2013) through nonlinear narration (Liu et al., 2010) that enables children to explore alternative story paths.

Scaffold Learning Support

There are certainly other media for presenting cybersecurity education that could appeal to young children such as cartoons, motion pictures, and videos. However, these media are less able to support individualized scaffolding, which are user selected through

interactivity, such as picture cues with illuminating text, or word pronunciation to assist with decoding text (Gissel, 2015). At the same time, interactive e-books allow security and privacy risks to be communicated in easy to imagine scenarios using metaphors and analogies that helps users to better anticipate outcome of their actions (L J Camp, 2009; Wash & Rader, 2011; Zhang-Kennedy et al., 2016, 2017). Interactive e-books enable the presentation of both positive and negative outcomes of security decisions through nonlinear storytelling based on children's selected events (associated with 'hotspots'). By showing how the same situation could unfold with either negative or positive safety outcomes based on the choices of the individual learner, these interactive narratives create the opportunity for children to critically consider the ramifications associated with their online actions.

Device Adaptation

The last argument for the viability of interactive e-books for teaching young children cybersecurity in preference to other presentation forms is the popularity of tablets amongst children. Tablets are the preferred mobile device for children due to their convenience, portability, and larger screen size, making interaction easier for young children (Bus et al., 2015; Schugar et al., 2013; Zhang-Kennedy et al., 2017). Thus, it makes sense that stories presented on tablets in the form of interactive eBooks are the primary source of storybook reading amongst emerging readers, especially those who may still be developing manual dexterity (Burnett, 2010; Bus et al., 2014). Tablets are therefore a good media choice for delivering interactive e-books focused on cybersecurity education.

Design Guidelines for Children's Interactive E-Book

Several works found that multimedia enrichments had positive effects on children's user experience (Colombo & Landoni, 2014), story comprehension, story retention, and language skills (C. J. Pearman, 2008; de Jong & Bus, 2003; T Gissel, 2015). The integration of nonverbal information and language facilitates memory storage, while the

Several authors proposed guidelines for creating well-designed interactive e-books. On a fundamental level, interactive e-books are formats for storytelling. Therefore, good story design is key for engagement with well-developed main character, setting, and plot. Along this perspective, Dünser and Hornecker (2007) argues that "the story itself determines whether a book is engaging". Accordingly, the authors recommend the integration of interactive sequences to advance the story plot with clear signals when interactive features are triggered citing that when sequences are not clear, "children tend to be confused on whether they have completed a sequence and needed scaffolding to try other interactive manipulation". In the same perspectives, other authors advocate for the strategic use of interactivity in e-books in a matter that supports learners to engage in relevant processes (Korat, O., Shamir, 2007; Schugar et al., 2013; Van den Broek et al., 2014). In particular, interactive e-books must be designed to support children's limited capacity to process information and their developmental needs (Hourcade, 2015; Mayer, 2014).

Other research points to the dangers of overdoing multimedia and interactive elements in e-books. Too much input, these researchers warn, can tax working memory

and distract from the main content, hindering attention and comprehension (Bus et al., 2014; Colombo & Landoni, 2014; Mayer, 2014; Schugar et al., 2013). At the very least, interactive e-book design must avoid 'seductive details' that disrupt learner's ability to focus on the important parts of the text, such as interactive hotspots that are placed "just for fun".

At a more granular level, Schugar et al. (2013) recommended four considerations for evaluating quality interactive e-books for young readers: (1) interactions should provide vocabulary and inference support; (2) supporting and extending interactions should outweigh purely entertaining interactions; (3) the time required to engage in interactions should be brief; and (4) interactions must be strategically placed to motivate without distraction from the overall message. Based on these criteria, Sandra Boynton's (2011*),"Blue hat, green hat"* is an example of a high-quality interactive e-book for beginning readers with a careful balance of interactions to motivate and engage readers over distractions. Additionally, the interactions are simple and brief such as drag and drop. Conversely, an example of a low-quality interactive e-book is Carisa Kluver (N.D.) *"The Three Pigs"* where the frequency and placement of sound effects at the end of each text snippet was reported as "annoying" and served no purpose to the storyline.

Widely accepted principles for designing multimedia instruction such as contiguity, coherence, personalization, and managed complexity (Clark & Mayer, 2012; Mayer 2014) also align with design considerations that are specific to child-computer-interaction: perceivability, operability, and developmental appropriateness (Hourcade, 2015). Perceivability refers to the clarity of an interaction's purpose before and after a

child engage with it. According to Hourcade (2015), this can be achieved by simplifying the user interfaces to consider children's limited "information processing, attention, and working memory" due to their developmental needs, using child-friendly language, and using recognition over recall to support children in extracting information. Similarly, operability refers to designing interfaces to be easy to use given children's physical and motor limitation, and providing appropriate affordances and constraints so that interactive elements are clearly distinguishable from static elements (Norman, 2013). Finally, developmental appropriateness refers to allowing for the children's appropriate level of information processing, attention, and working memory while also allowing children to see the outcome of an interaction and enabling an action to be quickly reversible when the outcome was not desirable (Hourcade, 2015).

And, of course, the design of quality interactive e-book for children should have the elements of classical story design, since the backbone for a story's engagement is dependent on a good plot, character, and setting. Interactivity within e-books should be used to advance the story line, helping learners to focus on the story's messages while minimizing distraction.

Conclusion

The literature is clear that children's exposure to online risks has risen to an unprecedented level, with mobile media usage tripling every three years, and now further accelerated by stay-at-home orders caused by the COVID-pandemic. Remote school and online socialization have become the new norm by which children learn and play, contributing to their online risk exposure. The literature agrees that early education is

needed to mitigate children's online risks of: exposure to inappropriate content; disclosure of private and personal information inappropriately; cyberbullying, and sexual exploitation.

Similarly, there is consistent evidence that cybersecurity education needs to be based on users' mental models of privacy and threats in order to communicate risk in easy to imagine scenarios with metaphors and analogies with the goal of improving users' ability to anticipate the outcomes of risky choices. With respect to young children, their understanding of online privacy and safety are underdeveloped and sometimes based on their experience with physical privacy. It is also unclear if experiences during the pandemic, with its dramatically heightened online experience, have affected elementary age children's mental model of online privacy and security. This thesis serves to bridge the gap by assessing whether the models of children's online privacy identified four years prior persists or has changed across time and culture, and to look at the short-term impact of exposure to an interactive e-book about privacy and security.

The first research question serves to extend the authors' findings by replicating the Canadian study to evaluate whether the online privacy knowledge, and decision making of children in the Eastern Coast region of the United States could be improved through an interactive e-book. To this end, the research questions investigated are as follow:

1. Can an interactive e-book be as effective in teaching online security to young children (aged 7 through 10) in the United States as it was in the study performed on Canadian children? If so, how do the results from both studies compare in

improving children's online security knowledge and privacy-decision-making behavior?

2. Did the current mental models of children's conceptualization of online privacy change or persist over time, culture, and location? Did the intervention of the interactive e-book change children's model of online privacy?

I am looking for measurable improvement in knowledge through the intervention of the interactive e-book by evaluating information retention and knowledge transfer. Children's engagement will be measured by the five subjective, self-reported criteria: 'fun', 'ease of use', 'ease of learning', 'character likability', and 'willingness to tell other kids'. Success would constitute that privacy knowledge improvement and engagement experience for the participants in the United States are comparable to that of Canadian children.

For the second research question, I am investigating if the current mental models have changed or persisted over the course of four years and across cultures, paying special attention to statements that reflect children's pandemic experience. While the geography offers additional diversity, it is recognized that the cultures of the United States and Canada are similar, being both North American countries. Therefore, the metaphors used to improve mental models in privacy and security within the e-book are likely to be understood in a similar matter by both populations. It is likely, therefore, that changes in mental model may be more driven by time passed rather than changes in culture.

Chapter 3: Methodology

Introduction

In this study, I conducted user studies of both parent and child. Parents were administered a questionnaire to see what is most important to them with regards to educational app about security and online privacy. I interviewed children before and after usability testing to assess their knowledge of security and online privacy. I remotely observed usability testing with parent and child co-reading an interactive e-book. I conducted a subjective satisfaction rating after the usability testing and collected open-ended feedback during post interviews from child and parent participants. Children engaged in a distractor activity between the usability testing session and their final interview, so that the final interviews could better test retention of the concepts explained in the interactive e-book. Post-distraction interviews also included questions about children's perception of their ideal world.

This chapter discusses my methodology, procedures, and evaluation measurements.

Research Design

This study replicated the study by Zhang-Kennedy & Chiasson (2016) to compare results in order to evaluate whether the online privacy knowledge of children ages 7-10 in the United States can be improved with an interactive e-book. Therefore, most of the questions were based on the original study. Additionally, one subjective quantitative criterion of 'educational value' was not measured in my study.[1] Other aspects of the

[1] The Canadian study included the subjective quantitative measurement of 'educational value' in the usability evaluation. This criterion was not measured amongst participants in this study.

research design that differed from the original authors are identified as the methods are presented in this chapter.

In my within-subject study, I worked with 15 parent and child (aged 7-10) pairs. The study instruments included: parental device criteria questionnaires, parents' child demographic and internet activities questionnaire, usability evaluations, children's pre and post privacy knowledge assessments, and a distraction activity. The session lasted approximately an hour for each pair. Sessions were conducted on a MacBook Pro laptop, controlled remotely by participants who joined the Zoom session using their own computers. The sessions were video recorded using Zoom web conferencing. Parent-child pairs were given control of the screen when they co-read the web version of an interactive e-book, "Cyberheroes" (https://www.leahzhangkennedy.com/ebook), during usability testing (Zhang-Kennedy et al., 2017).

Recruitment and Participants

I recruited a non-probability convenience and snowball sample within my personal network using social media, email, and phone. The total participants included 15 parent and child pairs. Participants were restricted to being residents of the United States. Parents were restricted to having a child aged 7 through 10. Children participants were restricted to being regular mobile devices users (e.g., at least 1 hour a day). Table 1 shows the demographic information for the parent and child pairs.

Parents were between the ages of 38 through 50, with 2 men and13 women. Ten parents had advanced degrees and five had bachelor's degrees. Three were stay-at-home

moms and the rest were working professionals. The mean age of the 15 child participants was 8.0 years old, with 5 boys and 10 girls.

Parent participants signed an informed consent form for both child and parent. Children gave verbal assent over video conference. Children participants received a $10 Amazon card as incentive for complete participation in the study.

Table 1

Participants Demographic Information

Parent Participant Code	Age	Gender	Child Participant Code	Age	Gender	City	State
P1	50	f	C1	10	g	Gaithersburg	MD
P2	44	f	C2	7	g	Potomac	MD
P3	39	f	C3	8	g	Rockville	MD
P4	45	f	C4	7	b	North Potomac	MD
P5	49	m	C5	7	b	Silver Spring	MD
P6	43	f	C6	10	g	Silver Spring	MD
P7	44	f	C7	9	g	Salvage	MD
P8	47	f	C8	7	g	Rockville	MD
P9	38	f	C9	8	b	Richmond	VA
P10	38	f	C10	7	g	Germantown	MD
P11	40	f	C11	8	g	Potomac	MD
P12	43	f	C12	9	g	Auburn	ME
P13	38	f	C13	7	b	McLean	VA
P14	45	m	C14	9	b	McLean	VA
P15	40	f	C15	8	g	Rockville	MD

Procedure and Materials

The procedure and materials are summarized in Table 2.

Table 2

Study procedure and materials

	Participant	Method	Material
Step 1	Parent	Survey questionnaire	Demographic & Device Criteria form (word document)
Step 2	Child	Semi-structured oral interview	Pre-knowledge assessment test
Step 3	Parent and child	Co-reading	"Cyberheroes" web application
Step 4	Child	Structured oral usability evaluation	Again-again table, Smileymeter
Step 5	Child	Distraction	Art supplies
Step 6	Parent	Structured oral usability Evaluation	Five-point likert scale
Step 7	Child	Unstructured post-distraction interview	Drawing
Step 8	Child	Semi-structured oral interview	Post-knowledge assessment test

Parents' Procedure

Prior to the session, parents completed demographic questions (age, gender, education, and occupation), and Child Background Questionnaires (age, gender, grade, device use, online activities, and prior training on cyber security). Parents also took a questionnaire based on a five-point Likert scale for the criteria they use in choosing educational children's apps. Criteria were ranked in order of increasing importance from

1 (being the least) to 5 (being the most). The criteria measured were: (1) 'fun', (2) 'age-appropriateness', (3) 'ease of use', (4) 'educational value', and (5) 'popularity ratings'.

For data analysis each participant was given an anonymous identifier. Children and parent pair were coded to identify child with parent as such: 'C1' to 'P1'.

During the session, the parent and child completed the usability testing, where they co-read the web-version of the interactive e-book with full control of the reading session. Afterwards, parents completed a post-usability evaluation, administered as an interview. Providing the post-test evaluation questions verbally rather than on paper was a more convenient and natural form of collecting data than a survey during a remote study. Using an interview approach also enabled me to ask follow-up questions.

The usability evaluation included ten questions, with seven based on a five-point Likert scale (5 being the most positive), and three open-ended questions. As previously mentioned, because the first research question is based on comparative measures of the effectiveness of the e-book between Canadian children and the children in this study, the study reused questions from the original researcher when possible for consistency. The seven questions measured: (1) age appropriateness, (2) enjoyment/fun, (3) ease of use, (4) effectiveness [as a learning tool], (5) willingness to read again, (6) ease of parent-child interaction, and (7) helpfulness in facilitating conversation. The three open-ended questions elicited feedback for design improvements. These three questions were: (8) "What did you like about the e-book? Why?"; (9) What did you dislike about the e-book? Why?", and (10) "What would you change about the e-book (if any)? Why?".

Children's Procedure

As outlined in the procedure and material table, children's sessions involved pre-knowledge assessment, co-reading, usability evaluation, distraction, and post-knowledge assessment.

The knowledge assessment portion was administered as a semi-structured interview based on hypothetical scenarios. There were a total of nine questions with a maximum score of '3' per question, 1 being poor, 2 being marginal, and 3 being acceptable. Scores were summed up to get a 'privacy proficiency' score of up to 27 points. The purpose of the pre-knowledge assessment test was to gain a baseline of the children's online privacy and safety knowledge.

The knowledge assessment questions were be used for qualitative analysis so there was more latitude to introduce new questions. This assessment had nine questions with five new questions designed for this study (i.e., questions 3,6,7,8, and 9), and the rest were reused from the original study. Four knowledge-based questions assessed children's conceptualization of online privacy, and five questions were behavior-based questions assessing children's decision making in security risk situations. Knowledge questions inquired about children's understanding of privacy and personal information.

Also, the method of administrating of the knowledge assessment differed from the original authors (Zhang et al., 2016b). I applied the technique called Mission from Mars where the researcher leads the children to believe that they are communicating with a Martian that would like to learn about their lives (Dindler et al., 2005). The purpose of this approach is to ease the difficulties that children sometimes have in fully

communicating about their contexts (Hourcade, 2015). This approach also alleviates the pressure from the child as the test subject by transferring the burden of successful understanding onto the Martian, whom the children were helping better understand online privacy.

The questions that I introduced are as follows. These questions were: (1) "How would you explain online privacy to the Martian?"; (2) "What could the Martian do to protect its privacy?", (3) "What type of personal information should the Martian keep private when going online?", and (4) "What could happen if the Martian did not have privacy online?".

There were five behavior-based questions using hypothetical scenarios to assess how children would respond to different types of online privacy risks. I designed four out of the five questions based on the identified topics in the Canadian study. Only question 5 indicated with (*) was explicated provided from the original study, and was reused in my study. All questions were based on the seven topics the Canadian study found relevant risks to children: (1) personal information, (2) online chatting, (3) location sharing, (4) cyberbullying, (6) passwords, (7) online trust, and (7) digital footprints.

These behavior-based questions were: (5*) "Your best friend wants to borrow your password to email a funny picture to a friend you both know. What would you do? Why?"; (6) "Someone you don't know sends you a friendly message. What would you do? Why?"; (7) "You want to download an app your best friend is using so you can play together. The app asks for your birthday and address. What would you do? Why?"; (8) "You're playing an online game and another player says something mean and rude to

you. What do you do? Why?"; and (9) "You're playing your favorite online game, but none of your friends are available to play. You get a message from the app saying that if you share your location, it can find local players in your area for you. What do you do? Why?"

The post-knowledge assessment test was administered after the distraction activity and the parent's usability evaluation. The post-knowledge assessment test repeated verbatim the pre-knowledge assessment test questions to see if there were changes in the children's response. The purpose was to measure learning effectiveness based on information retention. Qualitative analysis of the pre- and post-knowledge assessment test was performed to compare the participants' mental models about security and online privacy to those found in the Canadian study, and to see if these mental models were altered at all by the encounter with the e-book.

The usability evaluation was administered as a structured interview, after the parent-child pair had interacted with the e-book. The usability questions for the children were reused from the original study for quantitative comparative measurements. This portion of the session included a five-point Smileyometer and an Again-Again Table. The five-point Smileyometer contained five questions to measure the user experience of the interactive e-book code from 1 (for least positive) to 5 (for most positive). The questions asked were: (1) "How fun was the Cyberheroes e-book?", (2) "How easy was it to use the e-book?", (3) "How well did you learn from the e-book?", (4) "How likeable were the characters?", and (5) "How willing would you be to show the e-book to other kids?". Children's engagement was measured with an Again-Again Table (3 for 'yes', 2 for

'maybe', and 1 for 'no') by asking: (6) "Would you read the e-book again?". The same two open-ending questions were repeated for children to elicit their opinions: (7) "What did you like about the e-book?"; and (8) "What did you dislike about the e-book?".

Next, children had a distraction activity. This aspect of the study design differed from the original authors, who instead used a distractor of a week's passage in time, whereas my distraction session was approximately 10 minutes with an art activity as the distractor. It was not possible to schedule multiple sessions with participants during the pandemic.

The distraction served two purposes. First, it was necessary in order to measure information retention during post-knowledge assessment test. Second, the distractor activity kept the child occupied while I administered the parent's usability evaluation. Since testing was remote, it was not practical to have another researcher to help streamline the testing process. The entire remote testing required balancing the testing activities and materials for both subjects. The distraction activity lasted an average of ten minutes. The distractor involved children responding either by drawing or verbally to the question: "If you could create your own world to live in, what would that world look like? What would it feel like?"

I collected data from the children's distractor activity after parents had completed their usability evaluations. Data collection about the drawing was administered as an unstructured interview. It became apparent that some children were showing signs of fatigue, so the nature of the unstructured interview offered them a break. Children were eager to share and talk about their drawing. Children were asked to explain their world,

what was in it, who lives in it, and why it was needed. Patterns quickly emerged from these interviews that had implications on the field of security for children. The interviews were transcribed, and I applied emergent coding to sort the data into themes for analysis.

Exploration of Children's Mental Models*:* The results from pre- and post-knowledge assessments pertaining to the question, *"How would you explain online privacy to a friendly Martian?"* were selected as the most relevant for analysis to investigate whether children's conception of online privacy aligned with the Canadian online privacy models or whether their models differed. Results were transcribed and coded for all 15 child participants age 7 through 10. For data analysis purpose, participants were coded as c1('gender''age') where c1 = child participant 1 such that c1(b8) refers to child participant 1, boy of age 8.

To explore whether children's model of online privacy persisted over time, and a different culture and location, I combined both deductive and inductive coding to analysis the qualitative data. The first step was deductive coding, where I applied the pre-determined theoretical framework identified as the four models children' held of online privacy (Zhang et al., 2016): (1) to be alone; (2) to hide secrets/special things; (3) to keep things to yourself; and (4) to not talk to stranger. The interview script was transcribed, and a codebook was developed to systematically move through the data. Each category was assigned a color code.

During this process, I coded snippets from each participant interview. Each color code corresponded to one of the four pre-determined children privacy model: (1) 'to be alone'; (2) 'to hide secrets or special things'; (3) 'to keep things to yourself'; and (4) 'to

not talk to strangers'. Next, I applied inductive coding to analyze the remaining data set, which did not fit into the pre-determined categories. Inductive coding allows for discovery of patterns from the ground up without preconceived notions based on an existing theoretical framework. For the inductive coding process, I applied thematic analysis to look for emerging themes and patterns amongst the data set. The transcripts were then coded based on the themes and patterns that had emerged.

Conclusion

I collected a considerable amount of data from both parent and child pre- and post-assessments, usability evaluations, and interviews. Most interestingly, the qualitative distraction activity led to unintended discoveries about how children's perception of threats and their ideal world in the present time were affected by the pandemic. These findings can be used to design cybersecurity educational tools that are timely within the context of the pandemic.

Chapter 4: Findings

Introduction

For the first research question, which evaluated the effectiveness of the interactive e-book, the data analysis was conducted for all 15 parent-child pairs. However, during the initial synthesis it became evident that the design of the interactive e-book was not suitable for children aged 10 and was reported by parent and child participants as too juvenile. This confirmed the original authors intention who had designed and tested the e-book for children age 7 through 9. Therefore, the quantitative e-book results associated with the two child participants aged 10, e.g., parent-child participant 1 (P1, C1) and parent-child participant 6 (P6, C6), were excluded. Hence, the associated results for the first research question are reported for 13 children (aged 7 to 9) and 13 parents. For the second research question, which investigated the persistence of children's mental model of online privacy over time and culture, analysis and results were reported for all 15 children age 7 through 10.

Overall, the findings indicated that the interactive e-book (Cyberheroes) was effective in improving the online security knowledge of the child participants in this study. However, the children in this study had a much less positive response to the e-book when compared with Canadian children. The parents in this study also provided less positive ratings for the e-book than did their Canadian counterparts.

The more significant findings emerged from qualitative analysis of the children's responses to the pre- and post-knowledge evaluations and from the distraction activity. These findings indicate an evolution of privacy models compared to the Canadian study,

as well as significant evolution of one of those models. In addition, the themes that emerged shed light into how children's conceptualization of their physical and digital world have been impacted by the 2020 COVID pandemic. Collectively, the findings from both quantitative and qualitative results helped me to formulate conclusions, confirm design guidelines, and suggest next steps for future research.

This chapter discusses quantitative and qualitative results for parents, followed by quantitative and qualitative results from children.

Parents' E-book Evaluation

Quantitative Results

App Selection Criteria Questionnaire. Parents (n=13) were asked to rate the criteria they use when selecting educational apps, using a scale from 1-5 (with 5 being extremely important). The results showed parents ranked 'educational value' (M = 4.5) as the most important criterion for an educational app for children followed by 'age appropriateness' (M = 4.0) and 'ease of use' (M = 4.0). Parents' ranked 'fun' as third (M =3.7). The least important criterion amongst parents for choosing an educational app for children was 'popularity ratings' (M = 2.9).

Usability Evaluation. Parents evaluated the usability of the e-book on a five-point Likert scale, coded from least positive (1) to most positive (5), and the results are shown in Table 3. The parents' ratings were uniformly lower than the ratings from the Canadian study. 1 (least positive) to 5 (most positive) showed that the interactive e-book was moderately age appropriate (M = 3.8), and moderately effective as a learning tool (M = 3.9). More than a third of parents (5/13) felt that the "story didn't have much of a plot"

(P3). P4 said, "I felt I missed some pages at the beginning. It kind of jumps. The beginning wasn't very well explained as to how they became cyber heroes or how they recovered their cyber powers." They also found that the ease of interaction between child and parent was only moderately well designed (M = 3.2) and they rated the e-book as only moderately enjoyable (M=3.2).

In all seven measured categories (5 = most positive) parents in the Canadian study (Zhang-Kennedy & Chiasson, 2016) had a far more positive experience with the e-book with minimum score 4.1 and highest score 4.7, while the parents from the United States had the lowest score of 3.2 and highest score of 4.2. These numbers indicate that parents in my study only had a satisfactory experience with the interactive e-book (M=3.7) while those in the Canada study had a more positive experience (M=4.4).

Table 3

Comparison of Parents' Usability Evaluation median scores between the United States and Canada.

1= lowest median score; 5 = highest median score

	Age appropriateness	Fun	Ease of use	Effectiveness for learning	Ease of child/parent interaction	Facilitating conversation	Willingness to read again
United States	3.8	3.2	4.0	3.9	3.2	3.6	4.2
Canada	4.3	4.2	4.7	4.1	4.4	4.2	4.6

While some of this lower rating for the e-book in 2020 may reflect ever-higher expectations for interactive media, some of the difference in rating was clearly driven by the fact that most parent-child pairs did not discover most of the interactivity available in

the e-book. Interactive elements were marked by twirling translucent stars or by blinking translucent “hand” symbols (the icon that appears when someone mouses over a link). Several parents complained that these interactive elements were not accompanied by instructions or associated text. The most friction was experienced by a parent-child pair (P11, C11) who was unable to finish the story, because they thought the interactive e-book was a game where a task had to be completed before being able to advance to the next page. It is possible, but not guaranteed, that participants may have discovered these interactive elements more successfully on a tablet, where exploration is more expected.

Most parents thought the e-book was moderately helpful in facilitating conversation about security and online privacy (M = 3.6). The interactive e-book “helped as a guide to what types of questions and what things to point out to children about internet privacy” (P4). The e-book helped “to explain it [online safety] in a manner they could relate to and understand” (P13). Two parents did not find the interactive e-book helpful, “because we went over the material already” (P9) and “we had discussions about these topics and put rules in place so these things wouldn't happen, but if we hadn't, then it would be very useful" (P7). Most parents were willing to read the e-book again to their child (M = 4.2) and found the e-book easy to use (M = 4.0).

Qualitative Results

Open-ended feedback showed that parents clearly found value in the e-book: the interactive e-book had “timely topics on cybersecurity in light of the pandemic” and remote school (P8). The interactive e-book “covered all of the privacy issues in a simple way that’s easy for children to grasp the concept (P3), and “the characters appealed to

kids; everybody likes heroes" (P5). Those parents who were able to discover the interactive portions found it “fun” (P7) (P8). All parents agreed that to the book needed clearer signals about what you can do and where you can click.

Parents offered important suggestions to improve the content of the interactive e-book. Several of these suggestions reflect changes in common online activities since 2016. One parent suggested including the topic of safety while watching online videos, saying, “they like to watch videos so they need to know what they should do if they see something inappropriate and how to respond” (P15). Another parent felt that the topic of “chat rooms should be emphasized more, since they seem to chat more with friends than talk now” (P4). A parent also requested “a little more detail in each of the five categories” (P5). These suggestions also reflect the fact that when the content of this e-book is compared to the three categories of safety and privacy issues identified by Hasebrink, et al. (2009), content, contact, and conduct, the book does not address content issues.

The parent of a child participant aged 7, thought that the interactive e-book “could be a little more kid friendly, since the subject matter is still a little over his head”. The parent said: "For his age, he's just learning about passwords and stuff like that, and it's just because they started doing online schooling in the Spring [school went remotely due to 2020 COVID pandemic]. Otherwise, kids are used to logging on or tapping on an app and it starts right up.” (P5).

Children's E-book Evaluation

Quantitative Results

Pre- and Post-Knowledge Assessment. Figure 1 shows the total safety and privacy proficiency scores (maximum score = 27) per child before reading the interactive e-book (i.e., pre-knowledge assessment) and after reading the interactive e-book with distraction activity (i.e., post-knowledge assessment). These reported results are from thirteen child participants aged 7 through 9. As previously explained, results from Participants C1 and C6 were excluded from the analysis due to age. Each child participant's total score improved after reading the interactive e-book and after a distraction session. Based on the Central Limit Theorem, both data from pre- and post-knowledge assessments met the normal mean distribution curve for confidence interval calculation.

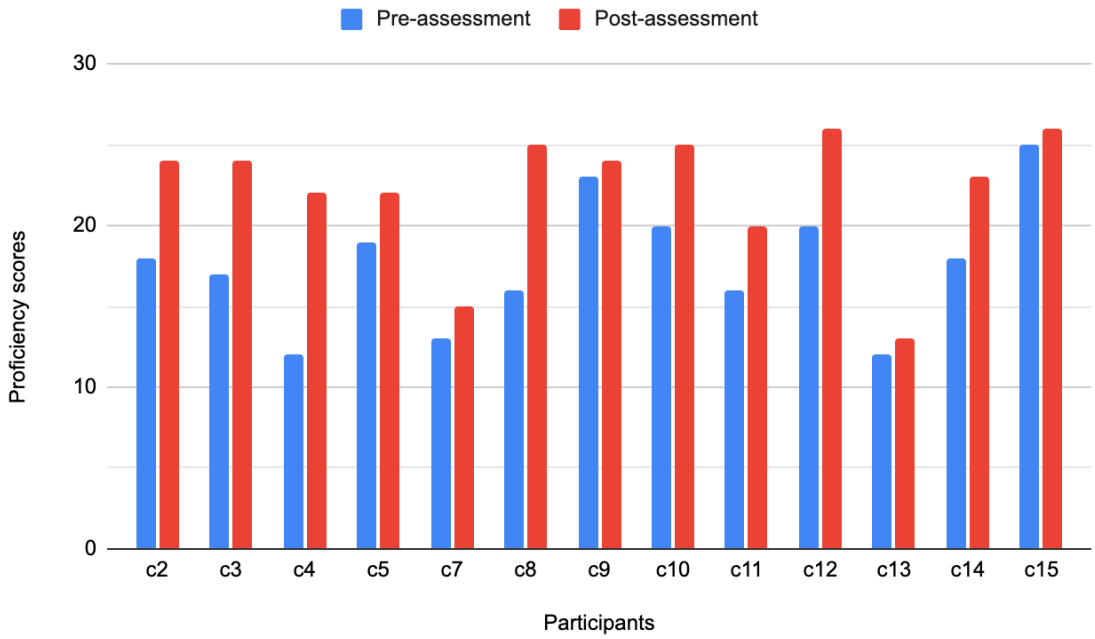

Figure 1. Total knowledge assessment scores per child in the study in the United States. (C1 & C6 data is excluded due to age.)

Figure 2 shows the mean knowledge assessment score with 95 % confidence interval for pre-assessment (i.e., before the reading session) and post-assessment (i.e., after the reading session and the distraction). The confidence interval was computed to investigate if there was a significant difference. The results show no overlap in the confidence intervals, indicating that there is at least 95 % confidence that the intervention of the interactive e-book made a difference in improving children's safety knowledge.

Figure 2. Mean assessment score for pre- and post-tests.

To further investigate the degree of statistical significance, I applied the T-test for two paired samples to determine the P-value for pre-assessment (i.e., before reading the e-book), and post-assessment (i.e., after reading the e-book). Statistical significance also held true for the T-test where both p-value for the one-tail test (p=6.0828E-05) and the two-tail test (p=0.00012166) met the criteria for statistical significance ($p \leq 0.05$). The results from this study also suggest strong evidence that the e-book was effective in improving children's safety online privacy knowledge and children were able to retain the information after 10 minutes distraction.

Children's Usability Evaluation. The children in this study responded less positively to the interactive e-book than Canadian children as indicated from the Again-

and-Again table evaluation score of 2.0/3 (n=13), while the score from the Canadian children was 2.6/3 (n=9) (Zhang-Kennedy & Chiasson, 2016). About half of the child participants (6 of 13) were uncertain if they would read the e-book again, while more than half of the children in the Canadian study (5 of 9) were certain they would re-read the e-book.

Consistent with this finding, usability evaluation results from the Smileometer (a 5-point Likert scale from 1-5, with 5 being the most positive), showed that children from the United States evaluated the e-book less positively than did the children in the Canadian study. Table 4 compares results from my study with the Canadian study. In four of the five rated categories, children from the United States had a lower mean score of 3.5 for fun, 3.5 for learning, 3.1 for likeability, and 3.0 for willingness to tell other children about the interactive e-book. Surprisingly, however, the children in this study and Canadian children both gave the e-book a mean rating of 4.4 in the Smileyometer evaluation in the fifth category for 'ease of use'.

Table 4

Summary of United States and Canadian children's Smileometer Mean Scores.

	Fun	Ease of use	Learning	Character likeability	Willingness to tell other kids
United States	3.5	4.4	3.5	3.1	3.0
Canada	4.4	4.4	4.1	4.1	4.2

Based on observations and follow-up responses during post-usability interviews, the mean score of 4.4 for 'ease of use' does not accurately reflect ease of use in terms of

interaction with interactive features, which is consistent with findings from parent's usability evaluation. Most child participants (8 out of 13 children) read the interactive e-book without interactivity and multimedia, since participants did not discover the interactive portions. For example, nine out of thirteen participants did not know that the stars can be clicked or what purpose they served. When asked what made the e-book easy to use, participant C5 said, *"because it was just clicking the forward arrow over and over again. I thought there would be more to it. Unless I was missing something"*. The e-book was easy to use, because *"you just flip through the pages"* (C12). These findings suggest that the mean score of 4.4 for 'ease of use' is based on participants' perception that the e-book was not meant to include interactivity.

Qualitative Results

Qualitative Analysis of Online Privacy Mental Models. Results from pre- and post-interviews before and after the intervention of the e-book, indicated that children in the Eastern Coast region of the United States four years later, and amid a pandemic, still held three of the four online privacy models identified in children in the Canadian study: 'to keep things to yourself', 'to be alone', and 'to hide secrets or special things', while the fourth model, 'do not talk to strangers', experienced some evolution. In this study, children's understanding of this model was more accurately expressed as 'do not trust strangers.' This evolution reflects a movement away from the "real life" conceptual model based on "not talking to" strangers that are physically present, toward a conceptual model more appropriate to the online world. Also, one new potential model was identified amongst children in this study— 'don't let anyone see you'.

Another evolution in mental models was observed between the Canadian study and this study. In the Canadian study, the most frequently held mental models were those most closely associated with the world outside the internet: "to be alone" (5 of 14 children) and "to hide secrets or special things" (3 of 14 children). But in this study, the model of 'to keep things to yourself,' the mental model that translates most easily into appropriate privacy decisions, had the highest count (12 of 15 children) in my study. A similar evolution can be observed in that the lowest accounted model held by children in this study was 'to be alone' (1 of 15 children), a model completely based on the world outside the internet. And while in the Canadian study the least frequent model was 'to not talk to strangers' (2 of 14 children), in this study the more advanced model of "do not trust strangers" was held by three of 12 participants.

Pre- and Post-Knowledge Assessments. As previously discussed in Chapter 2, knowledge transfer is a measure of the learners' ability to apply acquired knowledge to a similar context (near transfer), and to different situations (far transfer) (Zhang-Kennedy et al., 2017). Results from pre- and post-knowledge assessment suggested that children in the Canadian study and in the United States both demonstrated near knowledge transfer.

Children in the Canadian study also reported having far knowledge transfer to different scenarios after a delayed testing session one week later, whereas my study did not test for far knowledge transfer, since it was not feasible to bring children participants back for an additional round of testing. This study had only one testing session where the pre- and post-knowledge assessment was administered after a ten-minute distraction session that followed the co-reading session. Also, while both studies administered the knowledge assessment as a semi-structured interview, the United States study framed the interview using the Mission from Mars technique, which was not a technique employed in the Canadian study.

It is possible that the differences in the way the questions were presented between the two studies could have influenced children's responses. I will discuss the results of near knowledge transfer between the two studies.

Near Knowledge Transfer. Near knowledge transfer was measured in the Canadian study by the children's ability to explain *why* passwords should not be shared with a friend due to the risk that a friend could tell others their "personal stuff". However, the Canadian study did not explicitly report how many children within the study had near transfer, whereas most children (11 of 13 children) in this study demonstrated near knowledge transfer based on their explanation of why password should not be shared with a friend.

Within this group, children showed a developed understanding of why password needed to be safeguarded to protect personal information with some showing sophisticated problem-solving skills to circumvent disclosure of their password. For example, c9(b8) proposed to create a guest account for his friend instead of letting his friend use his password, because "I don't want them to see my stuff or have it." Overall, children were wary about trust, and anticipated potential betrayal from friends who might "ruin something [games]"; send mean pictures that would embarrass them; steal their password or give it to others. Some examples of these concerns can be seen in c12(b9) response: "I would not let them use my password, because it's my private information. She can be lying to me even if she's my best friend"; and c14(b9), "I would not give it to him, because it's private stuff that only I should know, and he might do something…can't trust everyone."

Only two children in the United States study did not provide evidence of near transfer, one of whom had dyslexia and deferred all decision making to her mom. The other – a boy (aged 7), said that he would share his password with family members. Most

children in the United States study demonstrated successful comprehension of the necessity for personal information security, with children articulating the perceived risk of deception from friends or others by misuse or infringement of their password and accounts.

Further discussion of these observed mental models of online privacy follows.

Observations about Online Privacy Mental Models. Results Table 5 shows total number of children's online privacy model within a category before and after reading the e-book. One child C12(g9) was unable to explain what online privacy meant. She was encouraged to say what she thought, and some clarifications was provided by rephrasing the question without priming, but the participant was still unable to explain the concept.

Her respond was: "I don't really know how to explain it". Another child had dyslexia, C7(g9), responded with, "I don't know what that means". Her mother explained what online privacy meant by providing the definition, which biased the child's answer. Both these children's data are not included in the pre-e-book intervention categories. Additionally, three children [C1(g10), C2(g7), C10(g7)] maintained their models while also adopting new models after reading the e-book.

Table 5
Privacy Models

	Current Privacy Models				Evolved Privacy Models	
	To be alone	To hide secrets/special things	To keep things to yourself	To not talk to stranger	Don't trust strangers	Don't let anyone see you
Pre e-book						
Count	1	1	9	0	0	2
Participants	c8(g7)	c13(b7)	c1(g10), c2(g7), c3(g8), c4(b7), c6(g10), c9(b8), c10(g7), c14(b9), c15(g8)			c5(b7), c11(g8)
Post e-book						
Count	0	2	12	0	3	2
Participants		c2(g7), c8(g7)	c1(g10), c2(g7), c3(g8), c4(b7), c6(g10), c7(g9), c8(g7), c9(b8), c10(g7), c12(g9), c14(b9), c15(g8)		c1(g10), c2(g7), c10(g7)	c5(b7), c11(g8)

Overall, defining online privacy is not easy for children even for those who showed sophisticated understanding of the concept. This challenge of definition is an aspect well recognized in the literature on cybersecurity for children (Kumar et al., 2017; Livingstone, 2006; Zhang-Kennedy et al., 2016). Accordingly, children in my study explained online privacy through mental models; three of which were the same as the Canadian study; one model which evolved positively when compared to the Canadian study; and one new model that emerged and was reflective of the present time.

Persistent Privacy Models

To keep things to yourself (12 of 15 children): This was the most persistent privacy model children held, with nine of fifteen children in this category before the intervention of the e-book, and twelve children after the intervention of the e-book. Before the intervention of the e-book, most children were able to explain why it was necessary to safeguard personal information. After the intervention of the e-book, all children were able to explain the safety implications of online privacy. Their explanations revolved around not giving account information, name, address, location, and age to prevent security and privacy risks. Children's main concerns with disclosure of personal information were with their accounts being hacked or being tracked by someone to their house.

One girl thought it was safe to share passwords with her best friend if she changed her passwords immediately afterwards. Others deferred to asking a parent for permission. These concerns are encompassed in an explanation by C1(g10): *"If they have to create a username or any information that someone can see, they should not use their first or last name for people to see, and they should be mindful of what they say online to not give too much information out online, because people could find where you live, and you might*

not even know who they are". Another example of this safety concern is evident in C6(g10)'s response: *"If someone bad on the internet found your personal information, and know that there's a Martian on the planet, they will tell the Martian removal and put him in an incinerator".*

Prior to reading the e-book, four children could not explain the importance of not sharing personal information and seemed confused. For example, one girl associated online privacy with "*creating a password and username to protect your privacy, like on your Chromebook you have a password and username that's private, and online privacy is that thing"* C10(g7). However, when asked how a password and username would protect privacy, her explanation contradicted her protective measures, and she seemed confused: "*Well, you're not using your own username and password to log into your Chromebook and your account. Your own username is used to getting into g-mail and your own Chromebook and…yeah."* C10(g7). More interestingly, one child, C4(b7), showed a strong sense of impending danger when asked how he would explain online privacy to the friendly Martian, but he could not give an explanation that warranted his reactions. This is illustrated in his response, "*You can't use my accounts so get out of here!"*. When asked why, the child responded with action as opposed to explanation with, *"I would take his laser gun and shot him*", even though the Martian was described as friendly.

To hide secrets or special things (1 of 15 children): One child, C13(b7), in this category associated online privacy with physical privacy, as was observed in the Canadian study. His explanation of online privacy involved, *"putting my special things in my toy box to keep it safe*".

To be alone (1 of 15 children): One child, C8(g7) in this category associated online privacy with not wanting to be disturbed when "*you want to be alone, you ask for*

privacy when you're going to the bathroom," and you can protect your privacy "by hanging up a do not disturb sign or put on headphones, so you can't hear noise like when you're at the library".

Although the models of 'to be alone' and 'to hide secrets or special things', were identified prior to reading the e-book, only one child in each category subscribed to these mental models. Additionally, after intervention of the e-book, the model 'to be alone' no longer persisted. Therefore, it can be postulated that this model may be less prevalent amongst children in the United States and may be readily susceptible to replacement. Conversely, the model 'to hide secrets or special things' had an increase of two children within this category after reading the e-book – a stronger indication of persistence.

Evolved Privacy Model

Don't trust strangers (3 of 15 children): While most children had safety concerns with a stranger tracking them to their house or being kidnapped, none of the children explicitly indicated that you should not talk to strangers online. Their protective strategy to protect against 'bad people out there' was to not easily trust strangers. A few of the older children (ages 9-10) reported creating accounts with fake birthday or names to protect their identity, while two younger children (ages 7-8) avoided posting themselves to YouTube, "so he [bad guy] doesn't know his everything" c4(b7).

This model focused more broadly on trust and less narrowly on not "talking to" strangers is better adapted for the online world than its earlier predecessor 'to not talk to strangers." This model also indicates that the child participants four years later and in a different location have a more sophisticated understanding of online safety than those in the Canadian study. It also reflects the findings previously discussed in the pre- and post-assessments findings, which found that most of the children in this study had an acute

awareness of online deception, and are less inclined to trust online actors, whether they be known friends or unknown users.

New Privacy Model

Don't let anyone see you (2 of 15 children): Children in this group associated online privacy with closing or not showing yourself to people online. One boy described online privacy as *"turning off his video or closing his browser tabs,"* to prevent people from seeing him or the sites he has visited. One girl's definition was "to not let anybody see you online" C11(g8). The same girl associated online privacy with private body parts. To her online privacy meant, *"to not post your privacy parts [private body parts] online for people to see"* C11(g8). She quickly realized that her explanation was for the Martian, and thought it would no longer apply because, "*he's a Martian so he doesn't have private parts."* These children's perceived threats were framed in the context of being watched inappropriately by viewers online.

This new mental model of "don't let others see you" was held before and after the intervention of the e-book by the same two children. In this regard, the e-book did not make a difference in these children's model of privacy. The most urgent insight within this group was from one child, who indicated an awareness of child pornography, which speaks to the dramatic increase in child sexual exploitation reported during the pandemic (INTERPOL, 2020). While it may not be practical under the climate of COVID to keep children from talking with every unknown user over the internet, it is critical to teach children not to trust strangers online as identities and motivates can be easily disguised and deceived. Furthermore, it is essential to teach children the associated warning signs of an online predator so that children can be aware of red flags, such as attempts to isolate the child to a private chat room or virtual space, questions about parental monitoring of

devices, request to send photos with escalating level of inappropriateness, and luring to meet in person.

Observations about Reading the E-Book. Open-ended feedback showed that children enjoyed the learning aspect of the interactive e-book All children found value in learning about the five rules of cybersecurity, and "what you should and should not do on the internet", One child learned that hobbies could also be considered personal information that could pose safety risks if shared with malicious actors. Prior to reading the e-book, all the children's examples of personal information were of personally identifiable information such as passwords, age, and address, but none had considered personal hobbies and interests as potentially sensitive information. An example is provided: "I didn't know you should not tell people your hobbies or other things. I only knew you shouldn't tell people email address, or your birthday" (C2). Other children appreciated learning "about privacy information that you need to keep secret" (C10). One child (C14) only liked the fifth rule that passwords should not be shared, because he doesn't know his password as his parents set his devices to "auto-check" login. Ironically, auto-check password poses a security vulnerability. Two children-aged nine (C12, C9) did not learn anything from the e-book, since they had learned these lessons from parents. However, even these children valued the lessons in the e-book, and some of the children indicated they would share the book with a friend who did not know cybersecurity.

Most children enjoyed the use of superhero characters to explain online safety. For example, "I like that all kids can have cyber powers and be cyberheroes just make sure they keep password and privacy stuff" (C15). However, one child (C9) was confused by the story and found that the use of superheroes, who broke all the five rules of cybersecurity, unrealistic. During the interview C9 asked: "How can they be superheroes

if they broke all the rules? It doesn't make sense!". Interestingly, the same observation that superheroes can make mistakes, and recover from poor decisions, appealed to another child (C11), who said, "I liked that they may have forgotten to not share their private information, but every problem has a solution, so they fixed it."

Although the children generally rated the information in the e-book positively, they had more mixed feelings about the interactivity—primarily because not all the children experience it. A couple of children expressed frustration and annoyance with the twinkling stars that made it "very difficult to read and was distracting" (C9), while another child kept saying "this is so confusing" (C11) as she was trying to figure out what she was supposed to do with interactive hotspots in the bedroom scene.

Children's positive feelings about learning online safety practices may reflect their emotional need for safety—specifically their increased desire for security in a precarious pandemic time. It is also possible that children were influenced by their awareness that the study was about privacy.

Observations from the Distraction Activity. Children were asked to respond either by drawing or verbal description to the question: "If you could create your own world, what would it be? What would it look like and feel like?"

Twelve out of thirteen children responded by drawing, while one child responded verbally (C14). Four overarching themes emerged from the activity: 'pandemic' (6 of 13 children), 'fun city' (4 of 13 children), 'video game land' (2 of 13 children), and 'desserts and candy' (2 of 13 children). Within 'desserts and candy' the sub theme of 'disease' and 'alone or just me' emerged, which also seem to reflect the realities of isolation and fear of diseases from the pandemic. Below are excerpts from C12's interview:

- C12: All the animals are gingerbread, and I am the only one that lives in it.
- Moderator: What would you do if you got bored and want someone to play with?

- C12: I would just carve them into children to play with or turned them into gingerbread, so they don't have diseases.

The most recurring theme was 'pandemic,' with six of thirteen children describing their ideal world to be: "like a normal place with normal feelings, and normal temperature and virus free" (C7); "the world would be exactly the same, but without the pandemic" (C14); "the world would feel sticky and normal…no pandemic" (C12). The sub theme of 'normal school' and 'big brain and technology' emerged within the theme of 'pandemic'. Two children said there would be a "place where people can go to school and learn" (C15) and "it would be just like the way it is now with normal school without the pandemic" (C10), while one participant (C4) characterized his world as being needed to be saved by technology, and people with "big brain". To demonstrate the implication of the COVID pandemic in C4's world, an example of C4's conversation is provided:

- C4: The world requires technology and big brain people.
- Moderator: Why do we need big brain people?
- C4: Because they help the spaceship. I don't know how, but they just help the spaceship.
- Moderator: Where is the spaceship from?
- C4: The spaceship is from earth. It escaped out of the dumpster.
- Moderator: What is the mission of the spaceship?
- C4: To go save Mars from war.
- Moderator: What does this world feel like?
- C4: It feels like a big brain. Soft and squishy and the size of the planet.
- Moderator: Anything else you want to tell me?
- C4: The big brain people stay at home.

- Moderator: How can they help the spaceship, if they are at home?
- C4: They have very long necks.

Children's envisioned ideal world was "a world without the virus," in which children equated the safe return to normal school with an end to the pandemic. Within this group, concerns were around diseases. One child (C4) described a world that needed to be saved by technology. Others desired the comforts and solace of games, fairy tales, and candy. Two children (C3, C12) wanted to live alone. Notably, the children who wanted their world to be "just me" had more than two siblings in the household. Thus, their desire for solitude may be an internalization of their pandemic experience, or perhaps a reflection of the lack of privacy many are faced with under stay-at-home orders during the pandemic.

These insights from the distraction activity demonstrate children's elevated awareness of risk and solidify their desire for safety. As the literature is consistent that children's experience of their physical world influences their mental models (Kumar et al., 2017; Zhang-Kennedy et al., 2016), recognizing how the present time of COVID has impacted children's risk perception, could serve as a starting point to inform future security education that is adapted to the pandemic landscape.

Conclusion

Overall, this study showed that the interactive e-book was effective in improving the child participants' online safety knowledge. However, children in the United States study rated the e-book lower in four of the five measured criteria than those in the Canadian study: 'fun', 'learning', 'character likeability', and 'willingness to tell other kids'.

Several factors related to device used, the remote testing conditions, and the evolution of e-book expectations between 2016 and 2020, could have contributed to the e-book's lower ratings. First and foremost, the interactive e-book was designed to be experienced on a tablet, specifically an iPad, which was the testing device used in the Canadian study. Children in my study read a web-version of the e-book, because the app was not available in the United States. It is likely, though not certain, that had children read the e-book on an iPad, they may have discovered the interactivity, which may have contributed to a higher rating for 'fun'. Additionally, testing for my study had to be conducted remotely due to safety requirements from the University of Baltimore Institutional Review Board prohibiting in-person testing. The inability to have a controlled environment for testing meant that participants could not be ensured a non-disruptive environment, since I could not control for family dynamics during testing. There were a couple of incidents were siblings walked-in during test session to ask their parent a question. These disruptions may have affected children's focus and impacted their responses. Lastly, another key factor that contributed to the lower ratings is that it has been over four years since the e-book was designed. Technology has changed as well as children's level of experience with technology. Hence the e-book was perceived as dated by some children. Also, children in this study had a more sophisticated understanding of online safety, and some children exhibited self-directed protective strategies, which were not reported in the Canadian study. For these children who were ready for more complex lessons, the e-book was too basic, covering lessons they had already mastered.

The study also identified some more substantive weaknesses of the e-book, which also contributed to lower ratings. Many parents and some children found that the story's plot was poor, and it did not feel like a complete narrative. Some parents had to invent

narrative elements when asked by their child about certain outcomes. Also, the main character was not perceived by a few children as well-developed or relatable, since they were unable to understand why a superhero would break all the rules. The safety lessons were recognized as important, but the lessons were not explained with enough details about the safety issues. In the present time of the pandemic, parents and children are poignantly aware of their need for more thorough explanations pertaining to online safety and privacy. Also, the e-book was not comprehensive, as there were relevant online safety risks that weren't covered. These topics included: (1) how to respond to bad content (sexual or violent); (2) how to be safe in video chats; (3) how to identify strangers; and (4) how to recognize predatory grooming. Although some of these risks were present when the e-book was designed, they have become more prevalent, while the safety issues of video chats (specifically, zoom-bombing), is a new risk that has arisen since 2016.

As discussed in the literature review, in order to truly teach children complex safety issues pertaining to identifying strangers, and recognizing grooming behavior from online actors, effective learning would require the use of non-linear narratives, while simultaneous leveraging the power of metaphors and imagery, to enable children to explore alternative story paths with either positive or negative safety outcomes based on children's selected actions. Such choice-based narratives would create a simulated experience of role-playing to help children practice critical-thinking, and context-sensitive decision-making (Kumar et al., 2017). Additionally, this approach can scaffold learning, and help children solidify and internalize safe security and online choices (Kumar et al., 2017; Schugar et al., 2013). This strategy of choice-based narrative has been proven effective and is consistent with the literature on how to communicate

security risk to affect positive cybersecurity decisions (L J Camp, 2009). Future study should explore the use of choice-based narratives in safety and privacy instruction.

The study also identified the evolution of children's online privacy mental models since 2016. With respect to children in this study, three mental models persisted; one model evolved, and one new model emerged. The models that stayed the same are: (1) to keep things to yourself, (2) to hide secrets or special things, and (3) to be alone; while a more sophisticated model of 'don't trust strangers' evolved from the model 'do not talk to strangers'. The model 'don't trust strangers' is better adapted for the online world and indicates that children four years later in the United States have grown in experience and awareness of online risks than their Canadian counterparts. It also confirms the strong relationship between children's awareness of threats and their motivation to enact protective strategies. In addition, the study identified a new model of 'don't let anyone see you', associated with video chats and conference. This is a new risk that has risen since 2016 and has been magnified since the pandemic. The study also showed that the interactive e-book was an effective intervention and resulted in positive changes to most children's mental models (7 of 15). Amongst the mental models that changed, six models were improved upon, and one less useful mental model did not persist after reading the e-book. Lastly, the study also recognizes the influences of the pandemic on children's risk perception with children's most strongly perceived threat being the pandemic and diseases. Children equated the pandemic as their adversary to their most sought after need— a normal world that is 'virus free' with normal school. These statements reflect children's desire for security, community, and strengthen their need for safety.

Chapter 5: Conclusion

Introduction

In this paper, I evaluated the effectiveness of an interactive e-book to improve online privacy and safety knowledge in children living in the Eastern Coast region of the United States and compared quantitative and qualitative results with those reported in the original study performed with Canadian children (Zhang-Kennedy & Chiasson, 2016). After analysis of quantitative data based on five measured usability criteria and pre-and-post privacy knowledge assessments, this study concludes that the online privacy knowledge of the child participants in this study showed statistically significant improvement in the children's ability to identify safer security decision-making-behavior after a ten-minute distraction activity. This study also found that, similar to the Canadian study, information retention and near-knowledge transfer were exhibited amongst most child participants. However, children in the United States had lower positive ratings from reading the interactive e-book than their Canadian counterparts four years earlier. Qualitative findings demonstrate that while both parents and children value online privacy and safety instructions presented on the media of interactive e-book, participants in this study four years later amid a pandemic have higher expectations for online education about safety and privacy. These higher expectations included a desire for more thorough online safety explanations, and for effective narrative with well-developed plot and good character development. These weaknesses of the interactive e-book were mentioned explicitly by multiple participants. Additionally, this study confirms that the interactive e-book was not comprehensive and did not address the relevant online risks of

content pertaining to: (1) inappropriate content, (2) video chatting or conference, (3) identifying strangers, and (4) recognizing predatory behavior.

This study also acknowledges that teaching children the concept of online privacy and safety practices is difficult, and draws on evidence in the literature in cybersecurity education to conclude that in order to teach children how to recognize predatorial behavior and to identify strangers or other malicious online actors, future work in children's online security education will require the use of choice-based interactive narrative, simultaneously leveraged with visual metaphors to enable children to explore alternative safety outcomes associated with their online decisions. This approach would provide a simulated environment for children to practice critical-thinking, scaffold learning, and help children internalize safe security choices by exercising context-sensitive awareness in their decision-making. The author hopes to engage in future work in this area.

This study also investigated the evolution of children's mental models of online privacy from 2016 to 2020 and within the cultural context of the COVID-19 pandemic amongst children in the United States. The study identified three mental models of online privacy and safety that persisted: (1) 'to keep things to yourself', (2) 'to hide secrets or special things', and (3) 'to be alone'; and one model that evolved from its predecessor— 'do not talk to stranger' that is partly based on the children's experiences in the physical world to a broader model better adapted to the digital world— 'don't trust strangers'. Additionally, one new model of online privacy was identified— 'don't let anyone see you'. This model may well reflect the present pandemic time with its ever-present Zoom

environment and is associated for some children with the risk of being watched inappropriately. This portion of the study concluded that the majority of child participants in the United States had a more sophisticated understanding of online privacy and protective strategies than did their Canadian counterparts four years ago. Also, this study applied deductive and inductive analysis to conclude that the intervention of the interactive e-book was successful in improving most participants online privacy mental models after reading the e-book. Only the two children who held the new model of 'don't let anyone see you' were not influenced by the e-book. This study recognizes that this pervasive danger of being physically seen is a relatively new risk that was less present in 2016 when the e-book was designed, and therefore it was understandably not taught in the e-book. Moreover, this study contributed to empirical findings attesting to the validity of interactive e-books as a potentially viable medium for teaching young children about online privacy and safety.

Lastly, this study illuminated some of the effects of the pandemic on children's risk perception—largely discovered through qualitative analysis of the distraction sessions. The study identified that overall, children in the study perceived the pandemic as their primary threat adversary to their mental model of an ideal world. For children that ideal world is a normal world without the pandemic or diseases, and a return to normal school.

This study concludes that future work on cybersecurity education for children would require communicating security risks and safety lessons adapted to the present pandemic time with an awareness that children's desire for safety and community has

been intensified. This urgent need for security may ease the hurdle of motivating children to enact necessary security measures, since children's strong desire for safety could motivate them to enact protective strategies to prevent further dangers to their world that has been threatened by the pandemic., as was observed in this small sample.

Recommendations and Future Work

To improve cybersecurity security education for children in the United States in the form of interactive e-books these are the proposed recommendations. First, set the stage for engagement through a well-developed storyline with an emphasis on a solid plot, and apply multimedia enrichment strategically to draw attention to the story's main messages while minimizing distraction to avoid taxing working memory. Second, adopt the lessons on cybersecurity that are timely with the current technology and challenges children face, since children understand and solve new problems through mental models based on their experience with the world. For example, the story should include relevant lessons on: (1) secure video conferencing to minimize risk of Zoom-booming; (2) signs associated with predatorial behavior so that children could respond defensively by reporting or blocking contact; and (3) protective strategies to respond to inappropriate content online.

Third, educational e-books about online privacy and safety should incorporate choice-selected-narratives, to allow children to learn by exploring the potential outcomes of their choices.

If I were redesigning this experiment, I would also redesign the knowledge assessment questions to better gauge children's ability to distinguish between physical privacy and online privacy with these questions: (1) "What is the difference between privacy on the internet and privacy when you're not on the internet?"; (2) "What does it mean to be safe when you're online?"; (3) "What does personal information mean when you're online?"; (4) "Why is it important to not tell others your personal information?"; and (5) "How can I tell when an information is considered personal and should not be shared?". For the scenario-based questions, I would include questions that cover the urgent risks of online predators, and video conference hijacking (Zoom-booming) that were not covered in the original study. These questions would be set up as: 1) You're playing an online game with unknown players, because none of your friends are available. You get a message from one player saying: "Hey cutie, I voted for you! You're really good at this game! You must have been playing for years. How old are you? Btw, do you want to go to a private chat room so you can tell me how you got so good, that way the other players won't know your secrets?" What would you do? Why?; and (2) "You're having your weekly Zoom meeting with a few of your close friends. One guest joins the meeting with the username of one of your friends, whom you did not include in the meeting invite. The guest has their video turned off." What do you do? Why?. It would also be interesting to test the effectiveness of the redesigned e-book for a test sample with more varied cultural characteristics, and to be able to test for far-knowledge transfer.

Contributions

My research contributed to empirical evidence-based findings on the effectiveness of interactive e-books as a tool to help children learn online security so that they may navigate online spaces more safely. Subsequently, it also adds to the recognized paucity of educational tools about online security for young children and research on children's perception of online privacy. The study also addressed a gap in research pertaining to investigation of children's mental model of online privacy specifically during the pandemic of COVID-19. Thus, this study has extended the body of work on children's mental models of online privacy. Although this research did not set out to investigate children's mental models of their desired world, the study was able to unearth findings that illuminated their primary fear and their imagined solace, as shaped by the pandemic. These insights could be used as a steppingstone to inform the design of future educational tools about security and privacy.

Limitations

There were many limitations on the study, including the small sample size, remote testing environment, platform differences, and shorter distraction. First, although 15 parents and 15 children completed the study, the results of children's age 10 were excluded for the first research question, because they were not within the targeted age range of 7-9 for the interactive e-book. My intention to widen the age range was to see if more children could benefit from online privacy knowledge improvement, but the illustration and simplicity of the interactive e-book was strongly rejected by these older children and was reported as not age-appropriate in terms of maturity level. Hence, my

sample size was less than ideal. While my results showed a statistically significant effect on short-term learning, the sample size was considerably smaller than that of the original authors (Zhang-Kennedy et al., 2017) with 22 parent-child pairs. Second, because of the COVID pandemic, the University of Baltimore's Review Board only allowed for remote testing so I could not control for testing environment with family dynamics during stay-at-home orders. Third, the remote testing requirement meant that I had to test on a web-version of the e-book on a desktop and not a tablet, since the app was not available in the United States. Four, as previously mentioned, the challenges of recruiting children participants limited my studies to participants that were within the United States, which culturally is very similar to Canada. Hence, the study was not successful at exploring mental models over varying culture. Fifth, due to practicality reasons, my distraction activity was considerably shorter (10 minutes) than the study performed in Canada, which had a distraction activity duration of one week.

Perhaps most significantly, my initial proposal for the study was to design my own prototype for the interactive e-book with content that would align with the times, and with some incorporation of choice-based narratives. However, this plan depended on being able to test with a paper prototype in person. When the pandemic made in-person testing impossible, the project scope had to be narrowed, resulting in this study, which was closely comparative to the Canadian study. This alternative study design depended on testing with the original prototype designed by the Canadian researchers.

References

Bennett, N., & O'Donohue, W. (2014). The construct of grooming in child sexual abuse: Conceptual and measurement issues. *Journal of Child Sexual Abuse*. https://doi.org/10.1080/10538712.2014.960632

Brewster, T. (2020). *Child Exploitation Complaints Rise 106% To Hit 2 Million In Just One Month: Is COVID-19 To Blame?* Forbes. https://www.forbes.com/sites/thomasbrewster/2020/04/24/child-exploitation-complaints-rise-106-to-hit-2-million-in-just-one-month-is-covid-19-to-blame/#a68a61c4c9cc

Buck. (2020). *COVID Webinar Series (TRANSCRIPT): Robert Redfield, MD*. https://www.buckinstitute.org/covid-webinar-series-transcript-robert-redfield-md/

Burnett, C. (2010). Technology and literacy in early childhood educational settings: A review of research. In *Journal of Early Childhood Literacy*. https://doi.org/10.1177/1468798410372154

Bus, A. G., Takacs, Z. K., & Kegel, C. A. T. (2014). Affordances and limitations of electronic storybooks for young children's emergent literacy. *Developmental Review*, *35*, 79–97. https://doi.org/10.1016/j.dr.2014.12.004

Camp, L J. (2009). Mental models of privacy and security. *IEEE Technology and Society Magazine*, *28*(3), 37–46. https://doi.org/10.1109/MTS.2009.934142

Camp, L Jean. (2009). *of Privacy and Security*. 37–46.

Christine R. (2020). Over-500-000-accounts-on-zoom-are-now-being-sold-on-hacker-forums-and-the-dark-web @ www.techtimes.com. *Tech Times*. https://www.techtimes.com/articles/248795/20200413/over-500-000-accounts-on-zoom-are-now-being-sold-on-hacker-forums-and-the-dark-web.htm

Colombo, L., & Landoni, M. (2014). A diary study of children's user experience with eBooks using flow theory as framework. *ACM International Conference Proceeding Series*, 135–144. https://doi.org/10.1145/2593968.2593978

Colwell, M. J., Corson, K., Sastry, A., & Wright, H. (2016). Secret keepers: children's theory of mind and their conception of secrecy. *Early Child Development and Care*.

https://doi.org/10.1080/03004430.2015.1031657

de Jong, M. T., & Bus, A. G. (2003). How Well Suited are Electronic Books to Supporting Literacy? *Journal of Early Childhood Literacy*. https://doi.org/10.1177/14687984030032002

Dindler, C., Eriksson, E., Iversen, O. S., Lykke-Olesen, A., & Ludvigsen, M. (2005). Mission from Mars: A method for exploring user requirements for children in a narrative space. *Proceedings of: Interaction Design and Children 2005, IDC 2005*. https://doi.org/10.1145/1109540.1109546

Druin, A., & Solomon, C. (1996). Designing Multimedia Environments for Children: Computers, Creativity, and Kids. In *Wiley Computer Publishing*.

Dünser, A., & Hornecker, E. (2007). Lessons from an AR book study. *TEI'07: First International Conference on Tangible and Embedded Interaction*, 179–182. https://doi.org/10.1145/1226969.1227006

Federal Trade Commission. (1998). *Federal Trade Commission*. Research in International Economics by Federal Agencies. https://doi.org/10.7312/schw92626-015

Ford, M., & Johnson-Laird, P. N. (1985). Mental Models: Towards a Cognitive Science of Language, Inference, and Consciousness. In *Language* (6th ed., Vol. 61, Issue 4). Harvard University Publisher. https://doi.org/10.2307/414498

Gissel, S. T. (2015). Scaffolding students' independent decoding of unfamiliar text with a prototype of an eBook-feature. *Journal of Information Technology Education: Research*. https://doi.org/10.28945/2317

Gordon, S. (2020). *Research Shows Rise in Cyberbullying During COVID-19 Pandemic*. Very Well Family. https://www.verywellfamily.com/cyberbullying-increasing-during-global-pandemic-4845901

Gregory, R. L. (1983). Forty Years On: Kenneth Craik's The Nature of Explanation (1943). *Perception*, *12*(3), 233–237. https://doi.org/10.1068/p120233

Hasebrink, U., Livingstone, S., Haddon, L. and Ólafsson, K. (2009). *Comparing children's online opportunities and risks across Europe: Cross-national*

comparisons for EU Kids Online.

Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. *Proceedings New Security Paradigms Workshop*. https://doi.org/10.1145/1719030.1719050

Hourcade, J. P. (2015). *Child-Computer Interaction*. https://homepage.cs.uiowa.edu/~hourcade/book/child-computer-interaction-first-edition.pdf

INTERPOL. (2020). *INTERPOL report highlights impact of COVID-19 on child sexual abuse*. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse

Jamie, P. (2020). Zoom-Bombing Will Not Stop Unless You Do This Says CEO Eric Yuan. In *Tech Times*. https://www.techtimes.com/articles/248523/20200402/zoom-bombing-will-not-stop-unless-you-do-this-says-ceo-eric-yuan.htm

Johnson-Laird, P., Girotto, V., & Legrenzi, P. (1998). *Mental models: a gentle guide for outsiders*.

Kaspersky. (2020). *How to Keep Kids Safe Online During the Coronavirus Outbreak*. Kaspersky. https://usa.kaspersky.com/resource-center/threats/internet-safety-for-kids-during-coronavirus

Korat, O., Shamir, A. (2007). Electronic Books versus Adult Readers: Effects on Children's Emergent Literacy as a Function of Social Class. *Journal of Computer Assisted Learning*, *23*(3), 248–259. https://doi.org/https://doi.org/10.1111/j.1365-2729.2006.00213.x

Kumar, P., Naik, S. M., Devkar, U. R., Chetty, M., Clegg, T. L., & Vitak, J. (2017). "No telling passcodes out because they're private": Understanding children's mental models of privacy and security online. *Proceedings of the ACM on Human-Computer Interaction*, *1*(CSCW), 1–21. https://doi.org/10.1145/3134699

Kumar, P., Vitak, J., Chetty, M., Clegg, T. L., Yang, J., McNally, B., & Bonsignore, E. (2018). Co-designing online privacy-related games and stories with children. *IDC 2018 - Proceedings of the 2018 ACM Conference on Interaction Design and*

Children. https://doi.org/10.1145/3202185.3202735

Liu, C. C., Liu, K. P., Chen, G. D., & Liu, B. J. (2010). Children's collaborative storytelling with linear and nonlinear approaches. *Procedia - Social and Behavioral Sciences*, *2*(2), 4787–4792. https://doi.org/10.1016/j.sbspro.2010.03.771

Livingstone, S. (2006). *Children ' s privacy online : experimenting with boundaries within and beyond the family Book section*.

Livingstone, S., & Bober, M. (2004). UK children go online: surveying the experiences of young people and their parents. *Online*.

Livingstone, S., Haddon, L., & Görzig, A. (2012). Children, risk and safety on the internet: Research and policy challenges in comparative perspective. In *Children, Risk and Safety on the Internet: Research and Policy Challenges in Comparative Perspective*.

Mayer, R. E. (2014). Cognitive theory of multimedia learning. In *The Cambridge Handbook of Multimedia Learning, Second Edition*. https://doi.org/10.1017/CBO9781139547369.005

Nolan, J., Raynes-Goldie, K., & McBride, M. (2011). The Stranger Danger: Exploring Surveillance, Autonomy, and Privacy in Children's Use of Social Media. *Journal of Childhood Studies*. https://doi.org/10.18357/jcs.v36i2.15089

Norman, D. (2013). *The Design of Everyday Things*. Basic Books.

O'Keeffe, G. S., Clarke-Pearson, K., Mulligan, D. A., Altmann, T. R., Brown, A., Christakis, D. A., Falik, H. L., Hill, D. L., Hogan, M. J., Levine, A. E., & Nelson, K. G. (2011). Clinical report - The impact of social media on children, adolescents, and families. *Pediatrics*, *127*(4), 800–804. https://doi.org/10.1542/peds.2011-0054

Oglethorpe, M. (2020). *The Modern Parent: Teaching Stranger Danger in a Digital World*. https://themodernparent.net/teaching-stranger-danger-in-a-digital-world/

Pavarini, G., de Hollanda Souza, D., & Hawk, C. K. (2013). Parental Practices and Theory of Mind Development. *Journal of Child and Family Studies*, *22*(6), 844–853. https://doi.org/10.1007/s10826-012-9643-8

Pearman, C., & Chang Ching-wen. (2010). CD-ROM Storybooks and Young Readers.

TechTrends, *54*(4), 52–57.

Pearman, C. J. (2008). Independent Reading of CD-ROM Storybooks: Measuring Comprehension With Oral Retellings. *The Reading Teacher*, *61*(8), 594–602. https://doi.org/10.1598/rt.61.8.1

Perner, J. (1983). *Beliefs about beliefs: Representation and constraining function of wrong beliefs in young children's understanding of deception*. *13*, 103–128.

Rideout, V., & Robb, M. (2019). The Common Sense Census: Media Use By Tweens and Teens. *Common Sense Media*, 1–104.

Schugar, H. R., Smith, C. A., & Schugar, J. T. (2013). Teaching with interactive picture E-books in grades K- 6. *Reading Teacher*, *66*(8), 615–624. https://doi.org/10.1002/TRTR.1168

Sharples, M., Graber, R., Harrison, C., & Logan, K. (2009). E-safety and web 2.0 for children aged 11-16. *Journal of Computer Assisted Learning*. https://doi.org/10.1111/j.1365-2729.2008.00304.x

Steeves, V. (2014). Young Canadians in a Wired World, Phase II: Life Online. *Media Smarts*.

Steeves, V., & Jones, O. (2010). Editorial: Surveillance, Children and Childhood. *Surveillance & Society*, *7*(3/4), 187–191. https://doi.org/10.24908/ss.v7i3/4.4151

T Gissel, S. (2015). Scaffolding Students' Independent Decoding of Unfamiliar Text with a Prototype of an eBook-feature. *Journal of Information Technology Education: Research*, *14*, 439–470. https://doi.org/10.28945/2317

The Common Sense: Media use by kids Age zero to eight. (2017). *Common Sense Media*, *47*, 1–36. https://doi.org/10.1007/978-3-319-01610-8

UNICEF. (2020). *Children at increased risk of harm online during global COVID-19 pandemic - UNICEF*. UNICEF. https://www.unicef.org/romania/press-releases/children-increased-risk-harm-online-during-global-covid-19-pandemic-unicef

Van den Broek, P., Kendeou, P., & White, M. J. (2014). Cognitive processes during reading: Implications for the use of multimedia to foster reading comprehension. In

Multimedia and Literacy Development: Improving Achievement for Young Learners. https://doi.org/10.4324/9780203892152-11

Wash, R. (2010). Folk models of home computer security. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/1837110.1837125

Wash, R., & Rader, E. (2011). Influencing mental models of security: A research agenda. *Proceedings New Security Paradigms Workshop*, 57–66. https://doi.org/10.1145/2073276.2073283

Whitten, A., & Tyger, J. D. (1999). Why Johnny Can ' t Encrypt : A Usability Evaluation of PGP 5.0 University of California Understanding the problem. *The 8th USENIX Security Symposium*.

Wisniewski, P., Xu, H., Rosson, M. B., & Carroll, J. M. (2017). Parents just don't understand: Why teens don't talk to parents about their online risk experiences. *Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW*. https://doi.org/10.1145/2998181.2998236

Zhang-Kennedy, L. (2013). *Improving mental models of computer security through information graphics*.

Zhang-Kennedy, L., Abdelaziz, Y., & Chiasson, S. (2017). Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. *International Journal of Child-Computer Interaction*, *13*, 10–18. https://doi.org/10.1016/j.ijcci.2017.05.001

Zhang-Kennedy, L., & Chiasson, S. (2016). Teaching with an interactive e-book to improve children's online privacy knowledge. *Proceedings of IDC 2016 - The 15th International Conference on Interaction Design and Children*, 506–511. https://doi.org/10.1145/2930674.2935984

Zhang-Kennedy, L., Mekhail, C., Chiasson, S., & Abdelaziz, Y. (2016). From nosy little brothers to stranger-danger: Children and parents' perception of mobile threats. *Proceedings of IDC 2016 - The 15th International Conference on Interaction Design and Children*, 388–399. https://doi.org/10.1145/2930674.2930716

Appendix A: Parental Consent Form

Whom to Contact about this study:

Principal Investigator: My-Linh Rouil
Department: SIAT
Telephone number: 240-593-5959

CONSENT FORM FOR PARTICIPATION IN RESEARCH ACTIVITIES
Teaching Online Security with an Interactive E-book for Children

I. INTRODUCTION/PURPOSE:

I am being asked to participate in a research study. The purpose of this study is to design better interactive e-books to help children learn about online privacy. I am being asked to volunteer because I am a parent with a young child aged 7-11 living in the United
States who uses a mobile device regularly. My involvement in this study will begin when I agree to participate and will continue until for up to an hour. About 20 people will be invited to participate.

II. PROCEDURES:

As a participant in this study, I will be asked to answer some questions about an interactive e-book and mobile devices. I will be asked to sign on to a remote video conference. My participation in this study will last for the duration of the study – approximately an hour. I will be video and audio recorded, but other personally identifiable information will not be included with results or response.

III. RISKS AND BENEFITS:

My participation in this study does not involve any significant risks and I have been informed that my participation in this research will not benefit me personally, but the outcome of study will benefit others.

IV. CONFIDENTIALITY:

Any information learned and collected from this study in which I might be identified will remain confidential with code numbers instead of names and will be disclosed ONLY if I give permission. The codes will be destroyed after data analysis is completed. All information collected in this study will be stored in a locked file cabinet in a locked room. Only the investigator and will have access to these records. Data collected as part of the research, even if identifiers are removed, will not be used or distributed for future research studies. If information learned from this study is published, I will not be identified by name. By signing this form, however, I allow the research study

investigator to make my records available to the University of Baltimore Institutional Review Board (IRB) and regulatory agencies as required to do so by law.

Consenting to participate in this research also indicates my agreement that all information collected from me individually may be used by current and future researchers in such a fashion that my personal identity will be protected. Such use will include sharing anonymous information with other researchers for checking the accuracy of study findings and for future approved research that has the potential for improving human knowledge.

Check if images or video are recorded during the research study:

☐ Yes, I give permission to use my image in scientific publications or presentations.

☐ No, I do not give permission to use my image in scientific publications or presentations

Check if voice recordings are used during the research study:

☐ Yes, I give permission to use my voice in scientific publications or presentations.

☐ No, I do not give permission to use my voice in scientific publications or presentations

Although your confidentiality in this study is protected, confidentiality may not be absolute or perfect. There are some circumstances where research staff might be required by law to share information I have provided. For example, if an interviewer has reason to believe a child or elderly person is being abused (or has been abused), the interviewer is required by Maryland state law to file a report with the appropriate agencies. Similarly, if I report that I have been abused in the past, the interviewer may also have to file a report. In addition, if I am threatening serious harm to myself or another person, it may be necessary for the interviewer to warn an intended victim, notify the police or take the steps to seek hospital-based treatment.

V. COMPENSATION/COSTS:

My participation in this study will involve no cost to me.

VI. CONTACTS AND QUESTIONS:

The principal investigator(s), My-Linh Rouil has offered to and has answered any and all questions regarding my participation in this research study. If I have any further questions, I can contact My-Linh Rouil at 240-593-5959.

For questions about rights as a participant in this research study, contact the UB IRB Coordinator: 410-837-4057, irb@ubalt.edu.

VII. VOLUNTARY PARTICIPATION

I have been informed that my participation in this research study is voluntary and that I am free to withdraw or discontinue participation at any time.

I will be given a copy of this consent form to keep.

VIII. SIGNATURE FOR CONSENT

The above-named investigator has answered my questions and I agree to be a research participant in this study. By signing this consent form, I am acknowledging that I am at least 18 years of age.

Participant's Name: _____ Date:

Participant's Signature: _____ Date:

Investigator's Signature: _____ Date:

(consent form template) – 12/02/14

Appendix B: Children Assent From

I, _____ understand that my mom, dad, caregiver, or guardian has said it is okay for me to take part in this study. I will help design new things that may help other children.

I am taking part because I want to. I have been told that I can stop at any time I want to. Nothing will happen to me if I want to stop.

Verbal assent was received by participate on _____ in the present of parent as a witness (mom/dad/guardian name) _____.

_____

Researcher's Signature

Appendix C: Parental Questionnaire and Device Criteria Evaluation

Parent's Demographic

1. How old are you?
2. What is your gender?
3. What is your ethnicity?
4. Where do you live? (city, state)
5. What is your highest level of education?
6. What is your occupation?

Device Criteria Rating

Please rank the following based on what's most important to you when choosing educational apps for kids where 1 is the most important and 5 is the least important ?

	1	2	3	4	5
fun					
age appropriateness					
ease of use					
educational value					
popularity ratings					

Child Participant's Demographic

1. How old is your child?
2. What is your child's gender?
3. What grade is your child?

Child Device Use & Background

1. What type of device does your child use?
2. What is your child's daily device use?
3. What are your child's primary online activities? (watching videos/YouTube, gaming, chatting, taking pictures, social media, school work, other - explain)
4. Has your child received formal privacy education/training?
5. Does your child have experience reading interactive e-books?

Appendix D: Interview Guide with Knowledge Assessment Questions and Usability Interview

Introduction [3-5 min]

[Greet participant]

Hi, my name is _____ and I am a graduate student at the University of Baltimore working on my Master Thesis in Interaction Design and Information Architecture.

First, I'm going to go over this form with you. It's called an **assent form** and you can tell me to let me know that you want to participate in this activity. We can stop at any time and nothing bad will happen if we do. If you don't want to answer any question, please just say so. Okay?

(explain key points - anonymity & recording)

I will be recording the session. Anything you tell me, and any video recording, will be seen by only myself. No recording of you will be shared with anyone, and nothing you tell me will be linked back to you.

No one else will have access to the videos. Once I review the videos, I will delete it.

The entire interview will take about an hour.

(parents should have already signed consent form for parent and child prior to interview)

<Have Participant Give Verbal Assent >

Thank you.

<explain process>

We are testing an interactive e-book, which will help children learn about online safety.

You will read the interactive e-book with your mom/dad as you normally would. I will ask you some questions before and after you read the e-book. We are testing the e-book design and not you or your ability. There is no right or wrong way to answer the questions.

Once you finish reading the e-book, we will do an art activity. Then we'll spend some time going over the questions again. Then you'll be done!

Do you have any questions for me before we begin?

<Parents questionnaire in file "parental questionnaire.docx" should have been completed prior to interview by parents.>

Child Interview Questions [3 mins]

We will begin with a few questions for some background information.

1. What's your favorite device?

2. What online activities do you like to do?

Children Online Security Questions [8-10 mins]

Now I'm going to ask you some questions based on imaginary situations.

"Imagine that there is a friendly Martian visiting Earth, and the Martian wants to go online."

< Knowledge based questions>

1. How would you explain online privacy to the Martian?

2. What could the Martian do to protect its privacy?

3. What type of personal information should the Martian keep private when going online?

4. What could happen if the Martian did not have privacy online?

< Privacy preserving behavioral questions >

(question 5 was reused from original study)

5*. Your best friend wants to borrow your password to email a funny picture to a friend you both know. What would you do? Why?

6.Someone you don't know sends you a friendly message. What would you do and why?

7. You want to download an app your best friend is using so you can play together. The app asks for your birthday and address. What would you do and why?

8. You're playing an online game and another player says something mean and rude to you. What do you do? Why?

9. You're playing your favorite online game, but none of your friends are available to play. You get a message from the app saying that if you share your location, it can find local players in your area for you? What do you do and why?

Co-Reading Activity [15-20 mins]

Now you and your mom/dad will read the e-book together. Please read the e-book as you normally would. Let me know when you're finished reading the e-book.

Usability Questionnaire [8 minutes]

Now, we'll see how reading the e-book went for you with some questions I will share with you on the screen.

(Parents should have already received the usability questionnaire form below, which they will fill out during this time with instructions to submit. Children will verbally answer usability questionnaires as I go over each question over screen share.)

Parents Usability Questionnaire

(Usability questions were reused from the original researchers study.)

Please rate question 1 through 7 by selecting only one answer:

1. How age appropriate was the e-book?

Not at all appropriate	Slightly appropriate	Moderately appropriate	Very appropriate	Extremely appropriate

2. How enjoyable was the e-book?

Not at all enjoyable	Slightly enjoyable	Moderately enjoyable	Very enjoyable	Extremely enjoyable

3. How easy was the e-book to use?

Not at all easy	Slightly easy	Moderately easy	Very easy	Extremely easy

4. How effective was the e-book as a learning tool for children?

Not at all effective	Slightly effective	Moderately effective	Very effective	Extremely effective

5. How willing would you read the e-book to your child again?

Not at all willing	Slightly willing	Moderately willing	Very willing	Extremely willing

6. How well did you and your child interact with the e-book?

Not well at all	Slightly well	Moderately well	Very well	Extremely well

7. How helpful was the e-book in facilitating conversation with your children?

Not at all helpful	Slightly helpful	Moderately helpful	Very helpful	Extremely helpful

8. What did you like about the e-book?
9. What did you dislike about the e-book?
10. What would you change to the e-book if any?

[end parent usability questionnaire]

<share screen showing children usability questionnaire and read out the questions to child participants>

Children Usability Questionnaire

1. Would you read the e-book again? (Yes, No, Maybe)

2. How fun was the e-book?

Super boring	Not fun	Kind of fun	Mostly fun	Super fun

3. How easy was it to use the e-book?

Super hard	Not easy	Kind of easy	Mostly easy	Super fun easy

4. How much did you learn from the e-book?

I didn't learn anything	I didn't learn much	I learned a few things	I learned a good amount	I learned a lot

5. How likeable are the characters in the e-book?

I didn't like them at all	I didn't feel anything for them	I like them somewhat	I like them	I like them a lot

6. How willing are you to show the e-book to another kid?

I will not show it	I don't know	I may show it	I will likely show it	I will definitely show it

7. What did you like about the e-book?

8. What did you dislike about the e-book?

9. What would you change about the e-book if any?

[end child usability questionnaire]

Distractor Activity [10 minutes]

Now let's do an art activity.

"If you can create your own world to live in, what would that world look like, what would it feel like?"

Instructs participants to draw or describe the world if they choose not to draw.

(Parents should have drawing/craft supplies readily available (pencil, crayons, paper etc.))

Children Online Security Questions [8-10 minutes]

Now we'll do our last round of questions. I'll be asking you again the same questions I asked you earlier. Remember these are imaginary situations.

< Knowledge based privacy questions>

How would you explain online privacy to the Martian?

What could the Martian do to protect its privacy?

What type of personal information should the Martian keep private when going online?

What could happen if the Martian did not have privacy online?

< Privacy preserving behavioral questions >

Your best friend wants to borrow your password to email a funny picture to a friend you both know. What would you do and why?

Someone you don't know sends you a friendly message. What would you do and why?

You want to download an app your best friend is using so you can play together. The app asks for your birthday and address. What would you do and why?

You're playing an online game and another player says something mean and rude to you. What do you do? Why?

You're playing your favorite online game, but none of your friends are available to play. You get a message from the app saying that if you share your location, it can find local players in your area for you? What do you do and why?

Wrap Up [3 min]

Is there anything else we haven't talked about? Did you want to say or ask anything else?

<Ask parents for comments or follow up. Check questionnaires and usability survey have been submitted by parents. >

Thank you. Seek any final feedback. Good bye.

Appendix E: T Test: Two Paired Samples

T Test: Two Paired Samples								
SUMMARY			Alpha	0.05		Hyp Mean Di	0	
Groups	*Count*	*Mean*	*Std Dev*	*Std Err*	*t*	*df*	*Cohen d*	*Effect r*
Pre-test	13	17.6153846	3.94838493					
Post-test	13	22.2307692	4.04462289					
Difference	13	-4.6153846	2.98715198	0.82848689	-5.5708601	12	1.54507861	0.84920778
T TEST								
	p-value	*t-crit*	*lower*	*upper*	*sig*			
One Tail	6.0828E-05	1.78228756			yes			
Two Tail	0.00012166	2.17881283	-6.4205025	-2.8102667	yes			