EasyChair Preprint

№ 66

Exploring Parents' Security and Privacy Concerns and Practices

Abdulmajeed Alqhatani and Heather Lipford

April 15, 2018

Exploring Parents' Security and Privacy Concerns and Practices

Abdulmajeed Alqhatani
University of North Carolina at Charlotte
aalqhata@uncc.edu

Heather Lipford
University of North Carolina at Charlotte
richter@uncc.edu

***Abstract*—Children today grow up within an environment with many digital technologies. Yet, the use of technology also brings with it the need to protect one's information and devices, and for parents, the need to protect their children as well. Previous research on children has mainly focused on addressing technology use among older teens, who are already primary users of many of the same applications as adults. Yet, little is known about the use of technology by younger children, and parents' perspectives regarding the privacy and security implications of that use. Through 20 semi-structured interviews conducted with parents of children aged 5-12, this study seeks to provide a clearer understanding of security and privacy related concerns, behaviors, and practices of parents and their children. We aim to expand the knowledge related to technology use in the family, and opportunities to improve how we protect and educate children in security and privacy.**

I. INTRODUCTION

Young children are now regular users of many different technologies [14, 16], with 57% of children in the US between the ages of 3 and 17 having access to the internet [2]. By the time they are twelve, children commonly own cell phones, with parents mediating their access to the internet. Many studies about children's security and privacy have focused on teenagers, who interact with a variety of applications including online games and social media. Yet, younger children also use technology regularly and may be at risk for a variety security and privacy problems, such as data leakage, phishing, and cyberbullying. Thus, we aim to explore the security and privacy needs of younger children and their parents.

We start this exploration by focusing on the perspectives of parents. We want to understand parents' concerns regarding the privacy and security of their children, the actions they take to protect their family's devices and information, and the actions they want their children to take. Our results will examine what issues parents are having regarding digital security and privacy, in order to inform the design of technologies or mechanisms that better meet their and their children's needs. Thus, our research questions are:

- What computer security and privacy concerns do parents have regarding their children's use of computing technologies and applications?
- What digital security and privacy practices do parents have that might impact their children?
- What digital security and privacy behaviors do children perform, or are encouraged to perform by their parents?

II. BACKGROUND AND RELATED WORK

Children are considered a special population, whose behavior and information are subject to additional protections not afforded to adults. For example, in the US, the Children's Online Privacy Protection Act (COPPA) sought to curb the information that websites collect from children under the age of 13. Thus, websites or applications targeted to children must adhere to those restrictions. As a result, many websites, such as popular social media platforms, restrict the age of their users to 13.

Even with these additional protections, there are still many digital security and privacy risks for younger children. Children can still be targeted for phishing attacks, their devices infected with malware, and their or their parents' accounts compromised. Data breaches can result in personal information about children being stolen. Children are a new target for identity theft [10], which may go undiscovered until they are older. And privacy breaches may lead to cyberbullying or even being targeted for attacks in the physical world [1].

However, much of the study of digital security and privacy needs and practices regarding children focus on teens. For example, previous studies examined family communication regarding technology use and online risks, and found that parents underestimate the important role of technology in their teens' lives [5, 13]. Teens view digital spaces as completely personal and private spaces [6], and parents and teens agree on the right of teens to have some privacy [7]. However, both also agree that this right should be limited [7]. Parents often use physical spaces, such as placing a computer in a family space, to define the boundaries in the digital ones [6].

Workshop on Usable Security (USEC) 2018
18 February 2018, San Diego, CA, USA
ISBN 1-891562-53-3
https://dx.doi.org/10.14722/usec.2018.23019
www.ndss-symposium.org

Another focus of previous research about teens is on the impact of technology controls on adolescent online safety. In this context, it was found that many technologies, such as mobile apps, have features that encourage parental control by monitoring and restricting teen's behaviors, rather than teen's self-regulation [11]. While direct parental intervention is helpful in reducing teens' exposure to online risks, it may negatively impact their ability to learn how to deal with online threats [12]. Thus, researchers suggest combining active parental mediation and direct intervention to protect children and to give them the authority to make effective privacy decisions [11, 12].

However, we know relatively little about the security and privacy implications of children's use of technology, and the needs for them and their parents for protecting themselves and their information. One exception is recent work by McReynolds et al. examining privacy issues with Internet connected toys. They interviewed both children and their parents to examine their perceptions regarding toys that record the child's conversation [3]. They found that children are not always aware that the toys can record them, and parents expressed concerns over what may happen to those recordings. They suggested improving communication with parents and children about the recordings to better inform their interactions.

The most similar study to ours is by Zhang-Kennedy et al. who interviewed parents and children regarding their perceptions on mobile device privacy threats [8]. They identified that children had a naïve understanding of privacy, such as being alone, keeping things to yourself, and not talking to strangers. They also saw substantial threats to their privacy from their peers or family members, which were different than parents' perceptions of threats of media and technology use more generally. The researchers used these results to inform the design of privacy educational materials [9], and a parent-child authentication mechanism [4]. We aim to expand on this work by examining technology use more generally.

III. METHODS

We conducted 20 semi-structured interviews with parents (12 mothers and 8 fathers) of children aged 5 to 12. Interviews were conducted between summer 2016 and spring 2017. Participants were compensated with a $10 Amazon gift card for their time after completing each interview. The participants were recruited through snowball sampling seeded from personal contacts on social media and email, asking contacts to share with their friends or forward to someone they thought would be interested in participating. Most (16) were completed over the phone, with four conducted in person. All interviews were audio recorded and transcribed.

The interview first focused on general computer usage by the family, and in particular the devices used by their children, and the activities performed with them. We then asked parents about their concerns regarding that technology usage, especially concerns related to security and privacy. We also asked participants about their concerns and behaviors regarding information about their children, and any actions they took to protect their families' information and devices. For instance, participants were asked what information they believe is being collected about their children, and what their kids do to protect their devices. Interviews lasted on average 20 minutes, and ranged from 8 to 38 minutes. Unfortunately, all but 8 minutes from the 10th interview were not successfully recorded.

Our goals were to examine the concerns and behaviors of both parents and children related to digital security and privacy. We utilized open coding to identify the patterns of responses of participants. Codes fell into three broad categories of technology usage and control, concerns, and behaviors, with specific codes being the different strategies or perceptions of parents and those they reported of their children. The code book was iteratively developed by an initial researcher using 12 interviews. A second researcher used that code book to re-code 5 selected interviews, finding the inter-rater agreement to be 88%. The second researcher then coded the remaining interviews with no changes to the code book.

Table 1: **Demographic information of the interview participants.**

Gender	Kids ages	Job
Female	2, 5	Stay at home
Male	9, 9, 10	Teacher
Female	10, 12	Small business owner
Male	8, 10, 12	Computer science professor
Female	3,6,7	Stay at home
Female	2, 8, 9	Spanish instructor
Male	8	Network services
Female	9, 13, 16	Marketing technologist
Female	12, 15	Physical Therapist
Female	11	Physical Therapist Assistant
Female	8,10	Nurse Anesthetist
Female	4,10	Nurse Anesthetist
Female	6	Nurse Anesthetist
Male	7,10	Anesthesiologist
Female	4,7	Homemaker
Male	5, 7, 10	Graduate Student
Male	8, 12, 14	Academic Researcher
Male	5, 10	Application System Engineer
Male	1,1,5, 7	Graduate Student
Female	11	Security Specialist

IV. RESULTS

Table 1 above reports a summary of demographic information about participants. All participants were from different families. We first discuss how our participants reported using technology, before going into more detail regarding their digital security and privacy.

A. Technology Usage

Parents reported that their children used technology for a variety of reasons, including to play games, watch videos, and browse websites, mostly educational websites. PCs, laptops, tablets, Xbox, and PlayStation were the most common devices used by children, many of which were shared amongst family members. Cell phones were mostly used by adults. Only three participants indicated that their middle school children have cell phones in order to be directly in touch with parents. Thus, unlike adults, children primarily use larger and less mobile devices. We also asked the participants what kinds of accounts and services their kids use. Only two participants mentioned that their kids have email accounts, and only two parents reported that their children have social media accounts (Instagram and Snapchat). These apps are used by kids mainly for posting personal pictures (e.g., sport pictures). No participant reported Facebook use by their children.

Parents reported a wider range of their own uses of technology, and we focused on the uses related to their family and children. For example, most reported digitally storing family-related documents, such as health records and school paperwork. Finally, we also asked about parents' use of social media. Thirteen participants mentioned that either one or both parents in the family use social media, mainly Facebook. Nine out of the thirteen share family and children's information over those platforms.

B. Technology Control

All of our participants restricted their children's access to technology in some way. One common strategy was to try and restrict technology usage to a certain amount of time, such as limiting device usage to 1-2 hour(s) per day, or for the most restrictive parents, to 1-2 hour(s) per week. Parents also reported rules regarding the time of day kids can use devices. For instance, one participant (P10) allows her kids to use their devices after school, while others mentioned times such as before dinner or at bedtime (P2, P9, P12, & P13). In addition, as expected, parents mentioned flexibility regarding those rules during weekends or holidays.

Many parents expressed similar sentiments regarding the kinds of technology and applications younger children should use. For example, all expressed opinions that young children do not need to use cell phones. Thus, only three participants reported that their middle-school aged children had cell phones. The same view was held towards email use. Parents reported that they utilized such restrictions in order to encourage the development of important skills on other activities. For example, P2 had the most restrictive attitude of all of the participants, as he believes that technology may hinder children's learning skills, such as reading and writing.

"All three of them are really strong readers because we limited their access to devices… You just see so many kids go out to a restaurant and parents are talking and kids are on their devices, or everyone in the family is on a device. So we're pretty unusual in that--and I think our children will be the first to complain about our stringent no-devices policy" [P2].

In addition to simply restricting screen time, parents also reported on strategies to control the activities on the devices by requiring permission or intervention by the parent. The most common method for doing this was by parents maintaining control with a password. Eight participants indicated that only the parents own the accounts and have the passwords for them. Thus, kids need to go through the parents in order to get permission to access or download material. Parents reported acting as an administrator for their children's devices, with the ability to deactivate or delete any account. While older children were sometimes allowed to have personal accounts and passwords, parents reported knowing the passwords and creating rules around usage, such as a rule against purchasing anything online without parental permission.

Few participants reported using technology specifically designed for restricting children's usage. For example, only two participants (P4 & P16) took advantage of filters and ratings to decide which apps were suitable for their children. In addition, browser settings were mentioned by two participants (P7 & P19) to allow them to block access to inappropriate content.

A final strategy was simply monitoring children–being present or knowledgeable of what their children were doing. For example, P7 indicated that he does not trust age filters and ratings, and instead tries to watch with his child: *"I just have to watch what he watches and if there's what I think is inappropriate I have to find a way to creatively, to show him why this is inappropriate…there's not a lot of teaching on that level"*. Another parent commented that she monitors her child's social media usage: *"I do have an Instagram account, but only to spy on my daughter."* [P9].

C. Technology Concerns

Most of the concerns driving technology restriction and control were not related to security or privacy. The primary concern, expressed by five participants, is the risk of exposure to inappropriate

content (e.g., pornographic or violent content). Another two participants indicated that some websites are not suitable for their children due to cultural and religious aspects. Technology addiction was another concern mentioned by two people. Technology is seen as a threat to children when technology use becomes a goal by itself rather than a tool to support children's different tasks. Another participant pointed out that the existence of massive amounts of devices today can weaken social relationships among family members.

The primary concern related to our focus is in revealing personal information online. This was a general concern regarding all kinds of technology usage, but parents focused on two particular kinds of applications. Six participants were particularly concerned with online games because they require users to enter private information, such as birthdates, location, email, payment information, etc. In this context, parents indicated that children are not mature enough to share this information.

My son likes to play a lot of games, he will go online and stuff. My biggest concern is that he will go online and talk with other players that are playing the same game online and give information or have other players get information from him" [P14].

Additionally, one participant prevented his children from playing games over the internet because he is worried that strangers may communicate with them.

Many parents were also concerned about social media, which is why all but 2 parents prevented their children from using any social media platform. However, parents themselves did report posting personal content about their kids and family on the web. In this regard, one of the parents expressed concern about tagging her kids' pictures by other people. Only three participants reported not sharing or posting any of their children's information online.

Two people expressed concerns around identity theft, which would be a concern but when their kids get older. Other security-related concerns were also rarely mentioned. Phishing, spyware, and malware were mentioned as other technology concerns by only three participants.

D. Security and Privacy Behaviors

As previously noted, many of the restrictions on technology use of children were not driven by security or privacy concerns. Yet, one of the most common strategies was authentication– using passwords to control what their children can do. For younger children, parents entered in passwords when needed. In certain cases, older children might have their own passwords, but must reveal those passwords to parents whenever asked:

If I need, you know, to go see something, I'm gonna know his password information, because he and I have that agreement that I can go any time and monitor to see what sites he is going to" [P20].

Thus, when it came to security and privacy-related behaviors, parents took on two strategies. The first was to do all of the security and privacy management themselves, from creating accounts, to protecting devices, to downloading applications. When asked about the methods their children used, parents in general responded that children at that age have a naive understanding of security and privacy. Thus, only parents undertake the burden of protecting their children's and their family's devices and information.

The second strategy to protect their children was to educate them regarding the rules for interacting online. Parents reported talking to their kids about potential threats, telling them relevant stories, and teaching them simple techniques to stay away from digital risks. The most frequent advice they gave their kids was a general warning about not sharing information online. For example:

"I just sat her down and asked if she remembered the scandal about 2 years ago where they got the photos from snapchat where everyone thought they would remain anonymous and never be out in public. All those pictures were out in public and she remembered, so I said "you may not put anything on Instagram that you wouldn't want your grandmother to see. She was like "yes mom"..." [P9].

Other parents were a bit more specific about the kinds of information, such as to never provide their real name and location when asked by an application:

I try my best to express to the oldest one, don't tell people where you live or where you go to school or where you dance because people can get access to this and try to come see you there, and you know there are bad people in the world. I know that people are watching so I just try to explain that to them." [P12]

However, no parents reported providing guidance on what would be considered security-oriented guidance, such as how to choose good passwords, talking about viruses or malware, etc. In other words, children were taught and involved in relatively few security and privacy decisions and practices.

Parents' security-related behaviors were similar to other studies of adults. For example, antivirus software is used by many participants on either some or all of their devices. Seven participants had Apple products, and they mentioned that Apple products are protected against viruses and other security threats: *"We have some kind of antivirus something on the*

Dell. On the Mac we don't really do that much, because I think they're supposed to be safer. We have passcodes on our phones, and on the iPad" [P2].

Parents reported a variety of digital information that they store, primarily photos stored on mobile phones and digital records stored on a personal computer. Five parents also reported using email or cloud storage for certain family records as well. Surprisingly, one participant never stored digital copies of his child's files, but keeps them in a cabinet with a lock.

"I am old-fashioned I have a folder in the file cabinet with a lock. It's too easy to hack into everything" [P7].

Parents also made decisions as to what information is provided to applications, what is shared on social media, and where child-related data is stored. Parents did clearly consider their child's data as more sensitive as their own, and did report consciously considering the amount of information they post regarding their children. For example, [P12] stated, *"I am careful to say something actively not that we are going to go do something. I don't publicly post anything personal."* Seven of the thirteen parents who use social media indicated that they took advantage of privacy settings to limit sharing to particular people, such as family members and close friends. Our results reflect those reported in a study on parents' use of social media [15].

V. DISCUSSION

Our findings reflect other studies regarding the variety of restrictions that parents place on their children's technology usage [5, 8]. While not driven by security or privacy concerns, these do still serve to limit the exposure of children to digital threats. However, while parents did report talking to their children about privacy concerns, and not revealing personal or identifying information online, there was little discussion of any other threats. In general, for younger children, parents are taking the primary responsibility for securing devices and accounts. This is perhaps a missed opportunity to help children understand, at their level, security and privacy strategies and begin to practice them with parental involvement.

Our interviews also demonstrated the extent to which parents think about and make rules for technology usage, and yet do relatively little of that for security and privacy. Even specific security practices, such as passwords and maintaining accounts, were used by parents more for safety and protection from age-inappropriate content than for protecting a device or information. One challenge may be that there is relatively little guidance for how to teach security and privacy practices, and few mechanisms to scaffold children into performing practices at their level. Yet, by the time they are teenagers, children are likely to be the primary users of many applications and faced with myriad security and privacy decisions.

Giving our sampling method, our population was likely more heavy technology users, and more technology savvy than the broader population. Still, even our technology savvy parents used relatively few filters, settings, or controls to help monitor or control their child's technology usage. And although the majority of parents in our study expressed concerns over the collection and sharing of information about their children, most still did in some way, indicating the needs for protecting all of that information.

VI. CONCLUSION AND FUTURE WORK

In this study, we examined the perceptions of parents regarding their children's digital security and privacy. When it comes to their children's use of technology, parents' decisions and restrictions are mainly driven by concerns over the appropriate use and content of digital applications. They try and protect their children from digital security and privacy threats primarily through their own decisions and practices, shielding their children from having to worry about such issues.

Children, however, may have different perspectives. Thus, the next step is to examine how children understand security and privacy, and what practices they have that have security and privacy implications. These results will help to inform the design of mechanisms that can help parents and children educate themselves, and work together to protect themselves and their information.

REFERENCES

[1] B. Donelly, "Children's safety at risk after multiple government privacy breaches," *The Age*, July 13, 2016. [Online]. Available: http://www.theage.com.au/victoria/childrens-safety-at-risk-after-multiple-government-privacy-breaches-20160713-gq52dl.html. [Accessed Mar. 19, 2017].

[2] Child Trends, "Home computer cccess and internet use," August, 2013. [Online]. Available: https://www.childtrends.org. [Accessed: Sep. 26, 2017].

[3] E. McReynolds, S. Hubbard, T. Lau, and A. Saraf, "Toys that listen: a study of parents, children, and internet-connected toys," *in Proc. of the 2017 CHI Conf. on Human Factors in Computing Systems, CHI '17*, ACM, Denver, CO, pp. 5197–5207, 2017.

[4] K. Hundlani and S. Chiasson, "No passwords needed : The iterative design of a parent-child authentication mechanism*," in Proc. of the 19th Int. Conf. on Human-Computer Interaction with Mobile Devices and Services, MobileHCI 2017*, 4-7 September 2017, Vienna, Austria, (p. 45), ACM.

[5] L. Blackwell, E. Gardiner, and S. Schoenebeck, "Managing expectations: technology tensions among parents and teens," *in Proc. Of the 19th ACM Conf. on Computer-Supportd Cooperative Work & Social Computing, - CSCW '16*, San Francisco, CA, pp. 1388–1399, 2016.

[6] L. B. Erickson, P. Wisniewski, H. Xu, J. M. Carroll, M. B. Rosson, and D. F. Perkins, "The boundaries between: parental involvement in a teen's online world," *Journal of the Association for Information Science and Technology*, *vol. 67*, no. 6, pp. 1384–1403, 2016.

[7] L. F. Cranor, A. L. Durity, A. Marsh, and B. Ur, "Parents' and teens' perspectives on privacy in a technology-filled world," *in Proc. in Tenth Symposium on Usable Privacy and Security, - SOUPS '14*, Menlo Park, CA, pp. 19–35, 2014.

[8] L. Zhang-kennedy, C. Mekhail, and S. Chiasson, "From nosy little brothers to stranger-danger : children and parents ' Perception of Mobile Threats," *in proc. of the The 15th Int. Conf. on Interaction Design and Children, IDC' 16*, ACM, Manchester, UK, pp. 388–399, 2016.

[9] L. Zhang-kennedy, "Teaching with an interactive E-book to improve children ' s online privacy knowledge," *in Proc. of the The 15th Int. Conf. on Interaction Design and Children, IDC' 16*, ACM, Manchester, UK, pp. 506–511, 2016.

[10] P. Anand, "Cyberthieves have a new target: children," *The Wall Street Journal*, January 31, 2016. [Online]. Available: https://www.wsj.com/articles/cyberthieves-have-a-new-target-children-1454295685. [Accessed Feb. 15, 2017].

[11] P. Wisniewski, A. K. Ghosh, H. Xu, M. B. Rosson, and J. M. Carroll, "Parental control vs. teen self-regulation: Is there a middle ground for mobile online safety?," *in Proc. Of the 2017 ACM Conf. on Computer-Supported Cooperative Work & Social Computing*, *CSCW '17*, Portland, OR, pp. 51–69, 2017.

[12] P. Wisniewski, H. Jia, H. Xu, M. B. Rosson, and J. M. Carroll, ""Preventative" vs. "reactive:" how parental mediation influences teens' social media privacy behaviors," *in Proc. Of the 18th ACM Conf. on Computer-Supported Cooperative Work & Social Computing*, *CSCW '15*, Vancouver, BC, Canada, pp. 302–316, 2015.

[13] P. Wisniewski, H. Xu, M. B. Rosson, and J. M. Carroll, "Parents just don't understand: why teens don't talk to parents about their online risk experiences," *in Proc. Of the 2017 ACM Conf. on Computer-Supported Cooperative Work & Social Computing*, *CSCW '17*, Portland, OR, pp. 523–540, 2017.

[14] S. Barkin, E. Ip, I. Richardson, S. Klinepeter, S. Finch, and M. Krcmar, "Parental media mediation styles for children aged 2 to 11 years," *Arch. of Pediatrics & Adolescent Medicine*, vol. 160, no. 4, p. 395, 2006.

[15] T. Ammari, P. Kumar, C. Lampe, and S. Schoenebeck, "Managing children's online identities: How parents decide what to disclose about their children onlin," ," *in Proc. of the 33rd Annual ACM Conf. on Human Factors in Computing Systems, CHI '15*, Seoul, South Korea, pp. 1895–1904, 2015.

[16] V. Rideout, "Zero to eight: children's media use in america," *Common Sense Media*, Fall, 2011. [Online]. Available: https://www.commonsensemedia.org/file/zerotoeightfinal2011pdf. [Accessed Sep. 25, 2017].