

RESEARCH PAPER

Digitally Mediated Parenting in Bangladesh: Reality, Dangers and Answers

Rumel M. Saifur Rahman Pir*, Md. Forhad Rabbi and M. Jahirul Islam

Department of Computer Science and Engineering, Shahjalal University of Science and Technology, Sylhet, Bangladesh

Corresponding author: rumelpir.student@sust.ac.bd

Received: 21 Sept., 2022

Revised: 25 Nov., 2022

Accepted: 03 Dec., 2022

ABSTRACT

The youth of Bangladesh is heavily reliant on their various technological devices. Children now have much more convenient access to a broad variety of applications and services relating to education, communication, and entertainment because of the widespread availability of mobile phones, laptops, and desktop computers. As a result, parents in Bangladesh are naturally concerned about the increasing privacy and security dangers their children face when they go online. There is a lack of research on how to equip children and their parents to take action to avert the risks of the internet, despite the fact that certain prospective prediction models have been established to indicate which children are at high risk of internet privacy and security problems. This study was carried out to assist address that informational vacuum. This article analyzes survey data from 383 kids (aged 6 to 17) and 311 parents (aged 25 and up) as well as in-depth interviews with 30 kids and 42 parents to determine the best ways to protect children's privacy and safety online. Following that, we combined the survey findings with the interview insights to see what kinds of direct and indirect behaviors parents and children engage in that endanger their privacy and safety. It was also found that children are becoming more susceptible to online dangers as a result of a breakdown in communication between parents and children regarding their use of digital devices, the proliferation of social media platforms, and other factors (such as online gaming, shopping, texting with strangers, etc.). It was also shown that parents who monitor their children's online behavior by, for example, imposing time limitations on their kids' device use, may greatly improve their children's online safety and security. The research finishes with seven measures parents may take to protect their children's privacy and safety online.

Keywords: Children, Digital Activities, Privacy, Security

Despite common use, "privacy" and "security" do not refer to the same thing^[12] when addressing children's internet use. In common use, "privacy" refers to "the extent to which an individual is able to manage, access, and exert control over personally identifiable information"^[23]. Children are protected from having their personal information shared with an unidentified third party without their agreement or that of their

How to cite this article: Pir, R.M.S.R., Rabbi Md. F. and Islam, M.J. (2022). Digitally Mediated Parenting in Bangladesh: Reality, Dangers and Answers. *IJISC*, 09(02): 83-95.

Source of Support: None; **Conflict of Interest:** None



parents under the terms of privacy rules. Similarly, privacy precautions prevent identity theft and data breaches involving minors^[26, 33]. But security refers to the measures taken to ensure that sensitive data is kept safe from prying eyes in the event of a data breach, leak, or cyberattack. Furthermore, the deployment of safety measures guarantees the safety of children when they use digital platforms^[40]. Children are especially vulnerable to cyberbullying, harassment, and other types of online abuse if they are unable to protect their privacy and security online^[15]. Many privacy and security issues, such as hacking and misuse of passwords, malware download, phishing, improper content access, and many more^[11], are frequently linked to children. Children's physical and mental health may be negatively impacted when their online privacy is violated^[7]. This may manifest as a variety of symptoms, such as despair, stress, increased anxiety, difficulty utilizing social media, sleep difficulties, and avoidance behavior. Their physical and mental well-being may be at risk if sensitive information about them became public knowledge. Because of the information the hacker stole, it's conceivable that both parents and kids may lose their social security benefits. It has been claimed^[8] that hackers have used children's confusion about the internet to steal their parents' financial information. The implications of unrestricted access to the internet, especially if it includes age-inappropriate material, on the developing brains of children cannot be overstated^[1]. There are two main types of dangers associated with internet use: content threats and contact threats^[18, 30]. Threats from technology and the internet^[13] and human error^[9] are two further examples. Commercial spam and targeted emails or adverts (treating children as active clients) are examples of content that represent a danger^[37]. Other forms of adult or abusive content include pornography, violence, pro-anorexia, and drug-related material. Loss of privacy, "sexting," cyberbullying, and "cyberstalking" are all terms that allude to the use of technology to harass someone, and "grooming" is the process by which an adult cultivates an emotional attachment with a kid for the intention of committing sexual abuse^[28]. A child's behavior might pose a threat if he or she engages in activities that are socially unacceptable or illegal, such as file sharing without permission or harassing other kids^[9]. Information security risks associated with computers and the internet include malware (programs designed to disrupt a system, gain access to computers, and steal private data), phishing (a technique for tricking a user into divulging sensitive information by pretending to be a reliable source), lost or stolen data, compromised passwords, and internet addiction^[5, 35]. Addiction to computers and the internet is a further risk. Today's parents have options for protecting their children from potentially hazardous content online, such as kid-safe settings and parental control software, but these solutions don't provide complete protection^[22].

1. Objectives

The improvement of children's online privacy and safety is one of the primary focuses of this paper, as well as one of its goals. As a result, it is essential to have a grasp of the risks to one's privacy and security that are posed by the internet, as well as how these risks influence children. In addition, the article makes an effort to provide suggestions for parents, with the goal of ultimately providing a more positive atmosphere for children when they are using the internet. The following is a condensed version of the goals that this paper aims to achieve:

- ❑ To identify the common digital privacy and security threats for children and to analyze the pattern of their effect on children.
- ❑ To understand the reasons for which the digital privacy and security of children is being compromised.

- ❑ To examine the role of the parents and to justify the responsibility of the parents to improve the digital world for their children.
- ❑ To ensure a more secure and safe online environment for the children by offering some recommendations to the parents.

2. Methods

The primary focuses of the research are children and their parents. The authors needed to collect data from both the children and their parents. The collection of research data from children and young people is challenging [8]. Hence mixed method of survey and one-on-one interviews were used for both the children and parents. Initially, 383 children's data were collected through a game-based app and one on one interview was conducted with 30 children. Afterward, through an online survey, the authors collected data from 311 parents and then semi-structured interviews were conducted with 42 parents.



Fig. 1: Android app 'Pi Play' to collect data from children

To collect survey data from the children, it was important to reach out to the children. The children might not be interested to answer too many questions in the survey, and they will not also like an orthodox survey. Keeping this in mind, an Android app was developed which was a type of game where the children were asked questions and given points after every answer. Two images of that game are shown in Fig. 1. There were quizzes and small games included too after a few questions and finally, the children receive a total point based on their performance. This gave the children a flavor of playing an android game where their answers to the questions were stored in the database. As the children would not like to answer too many questions, the total number of questions was restricted to 28 only. In the initial part they were asked about their demographic information like age, gender, school medium, etc, in the second part they were asked some privacy and security questions like who sets the password for them, whom they share the password with, who shares their devices, etc. and in the final part they were asked about how they feel about the privacy and security violations on digital devices, for example, did they ever face any threat or harassment online, did anyone force them to do or see something online, etc. The summary of the dataset is given in Table 1.

As all the authors are locally from Sylhet, Bangladesh and also live here for long, they have good contact with a few primary and secondary schools in the Sylhet region. The authors visited a total of 12 primary

and secondary educational institutions in Sylhet region which included 4 Bangla Medium Schools, 5 English medium schools (National Curriculum), 2 English Medium schools (British Curriculum), and 1 madrasa. The mobile devices installed with the Android app were handed over to children of 6 to 17 years of age and each student took an average of 10 minutes to play the game. The authors visited with several devices at each institution for utilization of time. This process took about 2 months and finally, a total data of 383 children were successfully collected through the game-based survey. Statistical analysis was then done on the collected data.

After the survey, semi-structured interviews were conducted with 30 children in order to compare the findings of the survey data with reality. The authors chose 8 children first from the neighborhood and the parents of these 8 children helped us to recruit the other 22 child participants for the interviews. All the interviews were semi-structured where the parents were not present besides the children during the interview period. The children were asked about their uses pattern of digital devices, their online interests, and more importantly regarding privacy and security aspects of the digital world. The interview participants were 6 to 17 years old and 15 boys and an equal number of girls were interviewed. Each interview lasted approximately 20 to 30 minutes and all the children who participated in the interviews were entertained with chocolates.

Table 1: Summary of data sets, both children and parents

Children Data Set	Parents Data Set
Number of Attributes: 28	Number of Attributes: 45
Demographic Questions: 4	Demographic Questions: 10
Privacy Questions: 6	Privacy Questions: 8
Security Questions: 13	Security Questions: 16
Activity Questions: 5	Activity Questions: 11

Designing appropriate questionnaires for the parent survey was crucial. After much work, the survey's 45 questions were ready for distribution. There were three sections to the survey's questions. At the outset, we asked them some basic questions about themselves, such as where they were from and how many kids they had. When it came to their children's online safety and privacy, parents were polled on their thoughts, attitudes, and beliefs in the second section. Finally, they were questioned about their children's use of the internet, namely how they talk to their kids about being safe online, whether or not they keep tabs on their kids' actions, and so on. The summary of the dataset is given in Table 1. A total of 311 guardians took part in the study. The authors conducted in-person surveys with a total of 42 parents while 269 participated online. Email and messaging apps like WhatsApp were used to disseminate the survey's questions to online participants. Among the parents, 139 were male, 170 were female and only 1 identified him/herself as other. They are from all eight divisions of Bangladesh where Sylhet has the highest participation with 136 participants. Parents from the capital city Dhaka stood second with 51 participants. Among the other divisions, Chottogram had 32, Barishal and Rajshahi 14 each and Mymensingh got 11 participants. Participants were very poor numbers from Rangpur and Khulna divisions, only 6 and 5 respectively. Out of 311 parents, 73 identified themselves as postgraduates, 140 parents identified them as graduates and 74 parents just completed Secondary School Certificate Examination (SSC). The gender of the children of these parents was almost equal with 158 girls and 153 boys. These children are from different age groups of 6-17 years. Among the 311 children of these parents, 185 go to English medium

schools which is 59.5%. 47 are from British curriculum and 138 national curriculum. 34% of children are from Bangla medium school and 6% only from Madrasa, the numbers are 105 and 20 respectively.

The authors performed statistical analysis on the survey data collected from the 311 parents. Then one-on-one interviews were conducted with 42 parents to compare the results of the survey findings with the views of the parents. Initially we recruited 10 parents from convenient sampling and these parents help us to recruit another 32 parents through snowball sampling. Finally, we conducted interview with a total of 42 parents who have children of 6–17-year age range.

3. Background Study

Both childhood and adolescence are crucial developmental stages because they mark the emergence of responsible risk-taking. At these times, young individuals are especially susceptible because they lack the cognitive maturity to fully see the connection between their actions and their outcomes^[14]. In addition, digital technology is increasingly present in children's daily lives, whether at home or at school^[27]. Youngsters spend a lot of time plugged into various technological gadgets, including smartphones, tablets, laptops, and "smart" playthings. There has been a similar surge in young people's use of digital technology since the COVID-19 epidemic^[3, 39]. These days, young people use their digital devices for everything from hanging out with friends to learning and communicating with teachers^[28]. As the number of users grows exponentially, so do parents' concerns about their children's privacy and security online^[22]. Concerns about privacy and security associated with the use of digital technology range from the abstract (such as surveillance and identity theft) to the particular (such as avoiding embarrassment or keeping one's schedule under control)^[31]. Most children and adolescents will be victims of cyber abuse, cyberbullying, or online threats at some point in their life, a problem that has increased with the widespread adoption of the internet and the rise of social media among young people. Several areas of young people's lives, such as their sense of security and privacy, are negatively impacted by the anxiety and danger they experience online. Despite the widespread belief that protecting kids' privacy and security online isn't a major issue^[2], research shows that parents can have a significant role in doing so. But, it is also the truth that parents cannot carry the entire burden alone if their children do not actively seek safety. Adolescents and younger children are less able to retain self-discipline and perform well in novel settings due to pressure from their peers and the intensity of their emotions. Adolescents are more likely to reject standardized risk treatments^[25, 38] due to their impulsiveness, sensation-seeking, thrill-seeking, and other individual characteristics.

Children's understanding of internet privacy and data sharing is an important topic for HCI researchers, who are regularly conducting studies on the topic. One research demonstrated that kids as young as 8 years old could understand some of the privacy implications of making data publicly accessible and searchable by using the visual programming language Scratch^[32]. For instance, they realized that there are privacy risks associated with collecting and storing data, that analyzing data calls for skepticism and interpretation, and that data contains assumptions and obfuscated choices. Another research indicated that kids aged 6-10 were aware that internet-connected devices might record and replay their conversations, but they didn't make the connection that other people could listen in^[6]. Children aged 5-11 showed a rudimentary grasp that material may be sensitive and should be shared only with trustworthy persons, according to another research. However, these young people showed a general lack of comprehension of more sophisticated issues, such as the implications of communication mediums on privacy and security^[34].

In sum, these findings demonstrate that some youngsters may have a rudimentary awareness of online privacy and security, but that they need further assistance from adults to guarantee these.

When it comes to instructing children on how to best safeguard their own identities and possessions, there is no better resource than the parents themselves. Some parents view instilling in their kids a concern for privacy and security as a long-term endeavor rather than a quick fix^[4]. The typical American internet adult can only correctly answer five of thirteen basic cybersecurity questions^[16], according to the Pew Research Center. People's cybersecurity abilities are influenced by a variety of demographic and life circumstances^[20]. While parents are an important source of knowledge for their children, they should not be expected to be the only guardians of their children's privacy and safety online. Changing children's online behavior to protect their privacy and security in the digital world is part of a larger effort to make the internet a safer and better place for everyone^[36]. Adults in a child's life may help keep them safe online by providing guidance^[24]. As children are the primary actors, what they do online can have a substantial impact on whether or not they remain safe and secure while engaging in routine digital tasks^[17,21,29].

4. Findings from Survey (Children)

From the statistical analysis, it was found that the online safety of children is closely connected with the number of hours they use digital devices. Higher the use, the greater the threat. Children who regularly share their digital activities with their parents and teachers are less likely to face security violations. In the case of harassment, proportionally a greater number of boys are facing online harassment compared to girls. It was observed that the children studying in Bangla medium schools suffer more than the children in English medium schools. The children are sometimes solely responsible for a few types of security threats. For example, children prefer to share their email passwords or device password with their friends which cost their privacy and security. Many children play online games, and they make online friends not known to their parents. Our analysis shows that these children who have friends not known to their parents suffer higher security threats. Some children regularly chat with people outside their close family which also increases their safety risks. Many children use social media like Facebook, Snapchat, etc. and some of them do it without the permission of their parents. They share photos, and personal information like birthdays, home address, and school information, and all these increases their chance of becoming the victim of online abuse and harassment. Some children download the app without their parent's permission and also do online shopping without their parents' concern. Our analysis shows that these children suffer more online privacy and security violations. Photo sharing is not only done by the children rather the parents and other members of the family regularly post the children's photos on social media and these photos are being misused by online predators. Parents are sometimes responsible for making children unsafe in cyberspace. It was found that many parents do not have enough knowledge about the threats and risks which may be faced by their children online. Hence, they do not talk to their children regularly and also do not have enough literacy about the privacy and safety settings of digital devices. Our analysis shows that the children of those parents who have good e-safety knowledge are less likely to face privacy and security issues. The role of educators cannot be ignored either. We have found that the children who have received some kind of safety and security training from their schools can handle their online privacy and security issues in a better fashion.

5. Findings from Survey (Parents)

Children are abused or harassed online. From our research, it was found that although children of all ages suffer from digital privacy and security threats, children aged 12-15 years are in the highest danger. 34 out of 64 parents having kids of that age range and who participated in the survey mentioned that their kids reported some kind of harassment or abuse to the parents. That is 53.13% of children of age 12-15 years report their parents regarding this discomfort. Surely there is a chance that many kids do not even share this with their parents and if all the children used to report to their parents then the number could be bigger. The reports from parents of 9-12 years age group children also reported a high percentage of privacy and security threats. Out of 111 parents participants who have children of age range 9-12 years, 47 reported their children mentioned or faced threat/harassment or abuse online, this is 42.34%. The same experience for the 6-9 years age range is a little lower; 30.30%. However, the age range above 15 years suffered less, 25% of these children suffered from privacy or security violations online. This is shown in Table 2.

Table 2: Privacy and security violation Vs children age

Age of the children	Children in Total	Privacy or Security Violated	Percentage
6-9	99	30	30.30
9-12	111	47	42.34
12-15	64	34	53.13
15-17	36	9	25

It can be observed that the children of age 6-15 are most likely to report abuse or harassment to their parents. Children's report to their parents also varies depending on their type of educational institution. 55% of parents of madrasa-going children reported their children were abused or harassed online while this percentage drops sharply to 40.95% for Bangla medium students and further drops down to 35.5% and 23% for English medium national curriculum and English medium British curriculum students.

It was observed that there is a direct relationship between the time spent by children on digital platforms with the possibility of being abused or harassed. Higher the time, the higher the threat. The parents were asked how long their children usually spent on digital devices per day, particularly online. They were supposed to choose between any of the following options: below 3 hours, 3-6 hours, 6-9 hours, 9-12 hours, and finally above 12 hours. A very small number of parents mentioned that their children spent more than 12 hours per day on average with digital devices and 80% of them mentioned that they were somehow harassed or abused online. Children who spend 9-12 hours daily on digital devices are also very vulnerable to getting abused. More than 54% percent of children in this category mentioned being harassed or abused. And the probability of being abused category who spend 6-9 hours daily is almost the same as the previous category. However, the harassment ratio drops as the number of hours spent online declines. 38% of children reported online harassment or abuse to their parents who are in the daily average use of 3-6 hours category and the rate further drops down to 29% in the category of children using digital devices from less than 3 hours. This is shown in Table 3.

Table 3: Privacy and security violation Vs children age

Time on digital device	Children in Total	Privacy or Security Violated	Percentage
0-3 hours	89	26	29.21
3-6 hours	124	47	37.9
6-9 hours	81	43	53.08
9-12 hours	11	3	27.27
More than 12 hours	5	4	80

From the survey, we have found that the parents who observe or restrict the digital devices use of their children and also who give time limits to their children for using digital devices get better results compared to the parents who neither observe nor restrict their children's use or give any time limits. Out of 68 parents who said they observe or restrict their children's use of digital devices and also give time limits to their children (Category A children), 38% of children of such parents reported online harassment or abuse. This percentage rose to 56.2% for the children of those parents who neither observe nor restrict their children's use or give any time limits (Category B children).

Although parents' observation/restriction along with imposing time limit does not have a significant effect on the mental health of the children. 73.5% of category A children said they do not face any kind of mental stress, pressure, or feeling lonely whereas 68.2% of category B children said they do not face any kind of mental stress, pressure, or feeling lonely.

Regarding photo sharing of children in social media, we have asked the parents to answer a few questions, for example, who shares the photo: The child himself/herself, the parents, or some other relatives or friends? It was observed that if nobody shares the photo of the children on social media then the probability of getting abused or facing harassment by the children is reduced by 17%. 41.4% of the children who either posted their photos on social media or their parents or anyone else posted their photos reported some kind of harassment or abuse where the rate is 36.2% while not the children or no one else ever posted the children's photos.

It was also observed that school training does not impact much in ensuring children's privacy and security online. 43.8% of the children who have received some kind of training from their educators (category C) reported being abused or harassed while 39.1% of children reported being abused or harassed while they have no such training (category D). This is a surprising result and the fact could be either the training is not focusing to the safety procedures to be followed by the children or maybe the category A students could report such discomfort to their parents properly while category D children are unable to understand the abuse or they are unable to report to their parents.

Parents may minimize internet abuse and harassment by talking to their children often. Our study questioned parents whether they address their children's internet activity often, occasionally, seldom, or never. Parents who routinely talk with their children have fewer mistreated or tormented children. Only 23.9% claimed their kids encountered internet abuse or harassment. This percentage rises to 52.5% for children whose parents never addressed this matter with them. When parents picked often or occasionally, 35.3% of their children had internet troubles, vs 47.3% when they indicated seldom or never. Abuse or harassment of children may be managed or lessened when parents discuss what their children are doing online, how they feel about this, etc. It was also observed that, educated parents regularly discuss with their children regarding their digital activities and either observe or restrict their children's online

involvement. Hence, it was seen that the parents who have higher academic degrees, their children suffer less privacy and security threats. This is shown in Table 4.

Table 4: Privacy and security violation Vs parent's education

Qualifications of Parents	Parents in Total	Privacy or Security Violated	Percentage
Post-Graduation	73	20	27.39
Graduation	140	51	36.42
Diploma	24	10	41.66
H.S.C	74	36	48.64

Child abuse and harassment can also be sharply reduced when the parents know how to handle the safety and security settings of digital devices as well as when they are confident that they can make their children understand these settings. Out of 311 parents who participated in the survey, 108 parents said they know about the safety and security settings of digital devices and also they can educate their children about this (Type E parents) and 89 parents said they do not know the safety and security settings of the digital devices and also they are unable to explain these to their children (Type F parents). For type E parents, only 25.90% of their children faced abuse or harassment online while this rate is above 66% for the children of type F parents. So to ensure the security and safety of the children, their parents can learn about the security measures of digital devices and particularly of the internet.

6. Findings from the interviews (Both Children and Parents)

The authors questioned a total of 42 parents and 30 children ranging in age from 6 to 17. The questions were asked in a semi-structured format. The children and their parents who participated in the study were selected using a combination of convenience and snowball sampling. We asked the parents to go out of the room while we were interviewing the children to give the kids the opportunity to speak without interference from their parents. The authors upheld the greatest possible ethical standards both during and after the interviews, and all of the participant's involvement in the interviews was entirely voluntary. It was discovered that the conclusions from the interviews closely matched the results of the survey. Having said that, there are a few noteworthy discoveries as well. For instance, throughout the course of the interviews, a few of the children disclosed that they make use of social media platforms such as Facebook, but their parents were unaware of this fact. A couple of the youngsters also indicated that they had a few friends with whom they were linked via online game-playing platforms and that they often talk with these less well-known pals while their parents are utterly oblivious to the fact that this is occurring. Apart from this, practically all of the children and their parents were of the opinion that increased communication between children and parents on their children's participation in online activities would help to lessen the threats to the children's digital privacy and security. Despite the fact that some of the children admitted that they do not talk to their parents about what they do online out of the concern that their parents will forbid them to use digital devices if they are aware of the dangers, the majority of the children said that they do talk to their parents about what they do online.

7. Recommendations

It was observed that if the children can make changes in the pattern of their digital use and act more sensibly in cyberspace, then their digital privacy and security situation would be improved. However, to ensure this, a few recommendations have been made by the authors for the parents and educators so that they can educate the children regarding these:

Firstly, caregiving adults like parents and teachers should be more friendly with the children regarding their digital activities. They should encourage the children to discuss with adults about their day-to-day activities online and should report it to the adults if they face any threat or are being harassed. Secondly, proper knowledge should be given to the children so that they can understand the safety threats associated with password sharing with friends and others. The parents can set the passwords for their children too and tell them to keep it secret. Thirdly, the parents should try to discuss the online friends of their children so that the number of online friends not known to the parents can be minimized to minimal or none. Parents and teachers should encourage the children not to share personal information, particularly their photos with unknown people during chatting or on social media. Fourthly, parents should restrict or monitor the unnecessary downloading or online shopping of their children, especially without the permission of the parents. And finally, parents and teachers should ensure proper online privacy and safety training and lessons for the children as it was found that the chance of becoming a victim of cyber threats is reduced significantly if the children have enough safety knowledge of how to protect themselves.

Limitations

Our research includes a few caveats. To begin, all of the interviewees come from the researchers' immediate and extended social circles (snowball sample). Second, most of the metropolitan institutions were chosen as survey sites. As a result, the comments might not be representative of the perspectives of rural youngsters. Finally, during tiffin or dismissal time, the kids would play the Pi game. Several of the kids may not have given careful consideration to the questions asked on both occasions because they were too eager to get the answers. Four, all the survey information comes from kids who are old enough to be in school. Some kids don't attend to school but nevertheless utilize computers and other electronics. It was not feasible for the authors to interview those kids. Finally, some of the parents who filled out the survey were only guessing at the answers to some of the questions.

CONCLUSION

The paper presented several crucial practices of children which are costing their online privacy and security. Using surveys and interviews, we investigated how children, and their parents may share certain responsibilities and behaviors to safeguard them from online safety risks. Initially, 383 children of Sylhet, Bangladesh supplied replies through a game-based Android application. Then a survey was conducted with 311 parents. Semi-structured interviews were also conducted with a small sample of children and parents. Ultimately, It was determined that certain online behaviors of children, such as chatting and sharing with strangers, sharing photos on social media, downloading or purchasing without parental consent, and sharing digital passwords with peers, make them vulnerable and insecure against different types of cyber-attacks. In addition, we have investigated how children may create a safer online environment for

themselves by avoiding concerns that endanger their privacy and security online, by addressing their cyber activities with their parents, and by obtaining sufficient guidance.

REFERENCES

1. Ahmed, S.I., Haque, M.R., Haider, I., Chen, J. and Dell, N. 2019. “Everyone Has Some Personal Stuff” Designing to Support Digital Privacy with Shared Mobile Phone Use in Bangladesh. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-13).
2. Ahmed, S.I., Haque, M.R., Haider, I., Chen, J. and Dell, N. 2019. “Everyone Has Some Personal Stuff” Designing to Support Digital Privacy with Shared Mobile Phone Use in Bangladesh. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-13).
3. Albuquerque, O.D.P., Fantinato, M., Eler, M.M., Peres, S.M. and Hung, P.C. 2020. A study of parental control requirements for smart toys. In *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (pp. 2215-2220). IEEE.
4. Ang, R.P. 2015. Adolescent cyberbullying: A review of characteristics, prevention and intervention strategies. *Aggression and Violent Behavior*, **25**: 35-42.
5. Boyd, D. and Hargittai, E. 2013. Connected and concerned: Variation in parents’ online safety concerns. *Policy & Internet*, **5**(3): 245-269.
6. Curtis, K., Roberts, H., Copperman, J., Downie, A. and Liabo, K. 2004. ‘How come I don’t get asked no questions?’ Researching ‘hard to reach’ children and teenagers. *Child & Family Social Work*, **9**(2): 167-175.
7. Cowie, H. 2013. Cyberbullying and its impact on young people’s emotional health and well-being. *The psychiatrist*, **37**(5): 167-170.
8. Crepax, T., Muntés-Mulero, V., Martinez, J. and Ruiz, A. 2022. Information technologies exposing children to privacy risks: domains and children-specific technical controls. *Computer Standards & Interfaces*, **82**: 103624.
9. Fox, A.K. and Hoy, M.G. 2019. Smart devices, smart decisions? Implications of parents’ sharenting for children’s online privacy: An investigation of mothers. *Journal of Public Policy & Marketing*, **38**(4): 414-432.
10. Gelman, S.A., Martinez, M., Davidson, N.S. and Noles, N.S. 2018. Developing digital privacy: Children’s moral judgments concerning mobile GPS devices. *Child Development*, **89**(1): 17-26.
11. Ha, Q.A., Chen, J.V., Uy, H.U. and Capistrano, E.P. 2021. Exploring the privacy concerns in using intelligent virtual assistants under perspectives of information sensitivity and anthropomorphism. *International Journal of Human-Computer Interaction*, **37**(6): 512-527.
12. Haber, E. 2020. The Internet of Children: Protecting Children’s Privacy in a Hyper-Connected World. *U. Ill. L. Rev.*, 1209.
13. Hautea, S., Dasgupta, S. and Hill, B.M. 2017. Youth perspectives on critical data literacies. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 919-930).

14. Hartikainen, H., Iivari, N. and Kinnula, M. 2016. Should we design for control, trust or involvement? A discourses survey about children's online safety. In *Proceedings of the The 15th International Conference on Interaction Design and Children* (pp. 367-378).
15. Jackson, S., Kelly, L. and Leslie, B. 2017. Parental participation in statutory child protection intervention in Scotland. *British Journal of Social Work*, **47**(5): 1445-1463.
16. Kostyuk, N. and Wayne, C. 2021. The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public. *Journal of Global Security Studies*, **6**(2): ogz077.
17. Kumar, P., Naik, S.M., Devkar, U.R., Chetty, M., Clegg, T.L. and 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.
18. Kumar, P.C., Chetty, M., Clegg, T.L. and Vitak, J. 2019. Privacy and security considerations for digital technology use in elementary schools. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-13).
19. Kumar, P., Vitak, J., Chetty, M., Clegg, T.L., Yang, J., McNally, B. and Bonsignore, E. 2018. Co-designing online privacy-related games and stories with children. In *Proceedings of the 17th ACM conference on interaction design and children* (pp. 67-79).
20. Kumar, P.C., Subramaniam, M., Vitak, J., Clegg, T.L. and Chetty, M. 2020. Strengthening children's privacy literacy through contextual integrity. *Media and Communication*, **8**(4): 175-184.
21. Lăzăroiu, G., Kovacova, M., Klietkova, J., Kubala, P., Valaskova, K. and Dengov, V.V. 2018. Data governance and automated individual decision-making in the digital privacy General Data Protection Regulation. *Administratie Management Public*, **31**: 132-142.
22. Liverpool, S., Mota, C.P., Sales, C.M., Čuš, A., Carletto, S., Hancheva, C., ... and Edbrooke-Childs, J. 2020. Engaging children and young people in digital mental health interventions: systematic review of modes of delivery, facilitators, and barriers. *Journal of medical Internet Research*, **22**(6): e16317.
23. Livingstone, S., Stoilova, M. and Nandagiri, R. 2020. Data and privacy literacy: The role of the school in educating children in a datafied society. *The Handbook of Media Education Research*, pp. 413-425.
24. Macaulay, P.J., Boulton, M.J., Betts, L.R., Boulton, L., Camerone, E., Down, J., ... and Kirkham, R. 2020. Subjective versus objective knowledge of online safety/dangers as predictors of children's perceived online safety and attitudes towards e-safety education in the United Kingdom. *Journal of Children and Media*, **14**(3): 376-395.
25. Magkos, E., Kleisiari, E., Chantias, P. and Giannakouris-Salalidis, V. 2014. Parental control and children's internet safety: the good, the bad and the ugly. *Proc. ICIL 2014*, **18**.
26. McNally, B., Kumar, P., Hordatt, C., Mauriello, M.L., Naik, S., Norooz, L., ... and Druin, A. 2018. Co-designing mobile online safety applications with children. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1-9).
27. McReynolds, E., Hubbard, S., Lau, T., Saraf, A., Cakmak, M. and Roesner, F. 2017. Toys that listen: A study of parents, children, and internet-connected toys. In *Proceedings of the 2017 CHI conference on human factors in computing systems* (pp. 5197-5207).

28. Odgers, C.L. and Jensen, M.R. 2020. Annual Research Review: Adolescent mental health in the digital age: facts, fears, and future directions. *Journal of Child Psychology and Psychiatry*, **61**(3): 336-348.
29. Olmstead, K. and Smith, A. 2017. Americans and cybersecurity. *Pew Research Center*, **26**(311-27).
30. Pir, R.M.R., Rabbi, M.F. and Islam, M.J. 2023. Applying a machine learning model to forecast the risks to children's online privacy and security. In *2023 International Conference on Intelligent Systems, Advanced Computing and Communication (ISACC)* (pp. 1-8). IEEE.
31. Pir, R.M.S.R., Rabbi, M.F. and Islam, J. 2022. Child engagement with digital devices during the COVID-19 epidemic in the global south: Are our parents and children equipped to make the best use of these? *Journal of Computer Science*, **18**(6): 509-519.
32. Reyna, Valerie F. and Frank Farley. 2006. "Risk and rationality in adolescent decision making: Implications for theory, practice, and public policy." *Psychological Science in the Public Interest*, **7**(1): 1-44.
33. Sewall, C.J., Goldstein, T.R. and Rosen, D. 2021. Objectively measured digital technology use during the COVID-19 pandemic: impact on depression, anxiety, and suicidal ideation among young adults. *Journal of Affective Disorders*, **288**: 145-147.
34. Singh, M. 2019. Compulsive digital gaming: an emerging mental health disorder in children. *The Indian Journal of Pediatrics*, **86**(2): 171-173.
35. Smithson, R. and Gibson, M. 2017. Less than human: A qualitative study into the experience of parents involved in the child protection system. *Child & Family Social Work*, **22**(2): 565-574.
36. Sun, K., Sugatan, C., Afnan, T., Simon, H., Gelman, S.A., Radesky, J. and Schaub, F. 2021. "They See You're a Girl if You Pick a Pink Robot with a Skirt": A Qualitative Study of How Children Conceptualize Data Processing and Digital Privacy Risks. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-34).
37. Tennakoon, H., Saridakis, G. and Mohammed, A.M. 2018. Child online safety and parental intervention: a study of Sri Lankan internet users. *Information Technology & People*, **31**(3): 770-790.
38. Yadav, S. and Chakraborty, P. 2021. Designing digital content for children: Understanding children's capabilities. *Childhood Education*, **97**(1): 75-78.
39. Zabatiero, J., Straker, L., Mantilla, A., Edwards, S. and Danby, S. 2018. Young children and digital technology: Australian early childhood education and care sector adults' perspectives. *Australasian Journal of Early Childhood*, **43**(2): 14-22.
40. Zhao, J., Wang, G., Dally, C., Slovak, P., Edbrooke-Childs, J., Van Kleek, M. and Shadbolt, N. 2019. I make up a silly name' Understanding Children's Perception of Privacy Risks Online. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-13).

