Usability, Security, and Privacy Recommendations for Mobile Parental Control

Vahiny Gnanasekaran
NTNU - Norwegian University of Science and Technology
Trondheim, Norway
vahiny.gnanasekaran@ntnu.no

Katrien De Moor
NTNU - Norwegian University of Science and Technology
Trondheim, Norway
katrien.demoor@ntnu.no

ABSTRACT

Current mobile parental control aids parents in monitoring their children's digital usage. Although many children are below 13 when receiving their first smartphone and social media accounts, only a few parents adopt such services. However, the literature reports several privacy, security, and usability challenges that need to be addressed to develop future mobile parental control. This paper presents three privacy, two security, and four usability recommendations for mobile parental control by conducting an in-depth literature review. 306 papers from the first iteration resulted in nine papers addressing clear recommendations and guidelines. Parental control should contribute to the children's digital skill set and the development of good online habits, in addition to addressing security and privacy controls for mobile applications.

KEYWORDS

parental control, recommendations, usability, security, privacy

ACM Reference Format:
Vahiny Gnanasekaran and Katrien De Moor. 2023. Usability, Security, and Privacy Recommendations for Mobile Parental Control. In *European Interdisciplinary Cybersecurity Conference (EICC 2023), June 14–15, 2023, Stavanger, Norway.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3590777.3590800

1 INTRODUCTION

Children of all ages are getting more familiarized with digital devices and online services. According to EU Kids Online 2020, European children between the ages of 9-16 spend 167 minutes daily on the internet on average, nearly doubling the amount in each country since the first survey was conducted in 2010 [31]. The COVID-19 pandemic has further increased the need for children to accept e-learning, digital classrooms, and video conferences as a part of their everyday life. Even though they display some understanding of privacy and security concepts [16], they still risk sharing sensitive information without fully comprehending the implications of doing so. Several popular social media applications (e.g., Facebook, Snapchat, TikTok) prohibit users under 13 years. Still, children below 13 possess their own social media accounts and smartphones [31]. The children's lack of risk awareness emphasizes the need for developing a proper digital skillset and intelligence.

A potential awareness tool in this matter is *mobile parental control*, which operates from the parents' smartphone and provides information from various digital services on the child's device. Recent studies show that the adoption of parental control tools in Europe has decreased on average from 28% [18] in 2010 to 22% [31] in 2020, despite the growing number of digital threats and risks that children may be exposed to. In general, the solutions are perceived to lack privacy and security controls [4, 8]. In addition, user studies report on "two-dimensional" functionality: they only fulfill certain aspects of technical features (e.g., time restrictions, content blocking, usage controls) without attending to the other unsolved demands, such as accounting for age and cultural differences, protecting sensitive information, and inducing digital independent thinking [19, 32]. How can future mobile parental control be implemented and designed, so that it has the potential to increase children's privacy and security awareness, along with parents' supervision and support? A partial answer might be available in this fragmented literature. Nonetheless, to the best of our knowledge, there are currently no studies providing a holistic understanding of the most important recommendations for mobile parental control solutions, by combining usability, privacy, and security considerations from the literature. This ensures a useful and compliant tool that both children and parents may benefit from.

Hence, this paper examines relevant requirements for mobile parental control within usability, privacy, and security, by conducting an in-depth literature review. The objective is to contribute to the design of the next generation of mobile parental controls: the applications should be secure and privacy-friendly, encourage the inclusion of both parents and children as contributors, teach children resilient online habits, and not only focus on the traditional perspective of restricting or monitoring access online.

2 BACKGROUND

This section briefly presents parental control and current privacy, security, and usability issues regarding parental control, while the findings from the literature review consider clear recommendations or guidelines.

2.1 Mobile parental control

Mobile parental control assists parents with supervising their children's smartphone use by granting them access to and limiting their children's usage of digital services [10, 21]. It is offered as an *integrated solution* in existing applications (e.g., streaming media, gaming, web browsers), or *dedicated solution*, which is available directly in the operating system (e.g., Android, iOS) [33]. Dedicated

EICC 2023, June 14–15, 2023, Stavanger, Norway
© 2023 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9829-9/23/06.
https://doi.org/10.1145/3590777.3590800

solutions possess multiple functionalities. Wisniewski et al. [33] discovered 42 unique features in the various applications in a qualitative analysis of 75 Android applications promoting parental control for adolescents. The most common setup was one mobile application for adolescents and a website or application for parents to monitor or edit restrictions. Some functionalities included watching and blocking web browsers, applications, and text messages. In addition, parents received an option to "seek help," which was not the case for adolescents.

2.2 Privacy Issues

Challenges regarding parental controls mainly concern two different, but equally important aspects of privacy. The first addresses the privacy required to use mobile parental control. Several regulations specify how minor data should be secured and managed to ensure data protection, such as the European General Data Protection Regulation (GDPR) [15] and the American Children's Online Privacy Protection Act (COPPA) [9]. GDPR and COPPA compliance is mandatory for all mobile applications collecting data. However, previous studies display significant privacy breaches in many popular parental control solutions [8, 22]. This is also reported by Reyes et al. [29], where several of the approved Google applications in "Designing for families" (i.e., program ensuring COPPA compliance) have multiple privacy breaches.

There are several reasons why developing companies struggle to adhere to privacy regulations. The need to receive verifiable parental consent from a child's device, and parents' unclear and vague rights in terms and conditions, by its nature, is often ignored [17]. For instance, managing a Google Play account requires the user to be above thirteen, excluding younger users, while COPPA regulation aims to protect children *below* 13.

The second privacy notion highlights the children's privacy against intrusion from their parents. Depending on age, parenting styles, and maturity, children should be aware of and act on the right not to tell everything. A US-based study [16] interviewed 26 children aged 5-11 and 23 parents about their strategies and "mental models" of online privacy and security. Their findings indicate that most parents are willing to preserve their children's privacy, but at the same time, they post pictures and other information about their children on their social media pages without consulting them or obtaining consent [16].Furthermore, parents defer explaining privacy concepts until adolescence since they do not assume their children are exposed to security and privacy concerns earlier [16]. Privacy against parent intrusion becomes more critical among teenagers [5, 14]. Cranor et al. [5] conducted semi-structured interviews of ten teenagers and ten parents of teenagers, showing that eight of ten teens identified parents inspecting their messages as unethical. In contrast, four out of ten parents believed the same. When parents use parental control applications on minors, whether teenagers or pre-teens, without sharing a common understanding of privacy, it may result in friction undermining the parent-child relationship.

2.3 Security Issues

Ali et al. [2] analyzed the security risks of some popular parental control solutions and found leakage of personal information and significant security vulnerabilities. The report discovered three of the 28 tested solutions do not encrypt user data on shared external storage that is accessible by any other apps with permission to access the SD card. Some examples of tested, dedicated parental control mobile software were FamiSafe, KidsPlace, and Life360. The latter shares the device position with a self-defined group and displays all positions simultaneously on a map for all group members. Data leakages and lack of authentication in such applications are more severe and exposed due to the nature of the data. Vulnerability analysis of parental control applications has also been performed [4, 22], indicating significant security flaws. The security issues imply that the current solutions should be upgraded in terms of applied technologies and permissions when managing data from children below 13.

2.4 Usability and New Affordances

Previous studies have initiated developing potential solutions to increase the trust between the parent and child. Two studies [12, 23] use a design approach to understanding the needs of the stakeholders and the parents. One of them developed an application named 'Circle of Trust' [12] with the perspective provided by 17 parent-child pairs with a mixed-method approach. This potential solution attempts to preserve the children's digital personal life and increase the trust-based relationship between parents and children. Their findings suggest that parents and children preferred Circle of Trust above other commercial parental controls regarding usefulness and ease of use.

Fuertes et al. [10] conducted surveys among parents, adolescents, and network administrators to determine how parental control applications are used and perceived. They identified best practices of the tools and mapped the actual threats and information adolescents face during web surfing without parental control. Their findings indicate that parents do not possess enough digital knowledge, and the adolescents were granted access to all web content through all devices, including institutional and privately owned devices. In [14] they report much of the same findings; ignorance of the tools and the difficulty in the application configuration were cited as the primary reasons for parents not adopting parental control.

Recent research has acknowledged the need to investigate the social aspects, along with technical understanding [3, 25]. The consideration for different parenting styles, ages, and contexts is essential to be aware of online risks and self-regulation and should be included in mobile parental control. Parental control should assimilate the technical aspects with the pedagogical perspective of understanding the safety and sharing practices and incorporation of such aspects into parental control solutions would enable new affordances.

2.5 Cybersecurity Awareness

However, due to the ever-changing technology and smart devices, many parents lack the proficiency and resources to educate their children about cybersecurity. Quayyum et al. [26] suggested collaborating with social or behavioral scientists to discover how to adapt cybersecurity knowledge to the skill level of parents and children. Their results display parents' concerns during children's digital interactions, such as online privacy, communication with

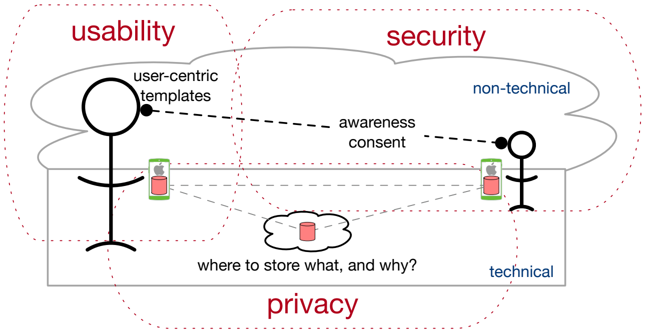

Figure 1: Parental (left) control of child/adolescent (right)

strangers, accessing adult content, internet addiction, and password practices. In addition, children struggle to comprehend the context and reasoning for sharing information. Proposed solutions were game-based learning, nudging tools, and adding cybersecurity to the school syllabus to increase awareness. However, parental control was not highlighted as a potential solution in this context.

As explained in this section, many aspects need consideration when developing better parental control solutions. Figure 1 depicts the interaction between the two users, parents and child/adolescent, and the areas that demand consideration from parental control. The literature demonstrates that parental controls should address security and privacy breaches to prevent misuse and extensive data collection. It should favor a balance between the parents' responsibility and not neglecting the children's private life, and consider the children's age and maturity, along with the parents' parenting style and knowledge level. However, the literature is still missing a holistic overview of the relevant recommendations to develop and design future parental control solutions, which is the main motivation underlying this work.

3 METHODOLOGY

This section briefly explains the in-depth literature review conducted to elicit parental control recommendations from the literature. The literature search was performed directly in the specified engineering/computer science web libraries and using internal library services. Journals/libraries within social science (e.g., child psychology, education) were excluded, due to the scope and the project's time limit. The search keywords were carefully selected to reflect the objectives of the literature review. Google Scholar was used to validating the search keywords. In addition, an iteration before finalizing the search strings collected 36 papers. The advantage of only including existing recommendations is quickly systemizing the present literature, and providing an overview of the research area. Table 1 contains the final search keywords, libraries, and search phrases applied for the literature review. The number in the brackets indicates the number of relevant papers found in the respective libraries.

The dataset contained 304 articles collected from the queries from the three libraries in the first iteration. The timeline was defined from January 2015 to March 2022 to highlight the latest developments in parental control technology. The initial screening was based on the title and abstract. For instance, smart toys for children (i.e., physical toys benefiting from online functionalities to enhance physical activities [6] and because of that also introducing potential security and use-related challenges and risks) were eligible for inclusion. Table 1 displays the total results from the three libraries, where 15 papers with recommendations were selected. Then, all papers without any explicit and well-defined lists of recommendations or guidelines, framework, or findings from empirical research were excluded by two reviewers. For instance, Ghosh et al. [11] was excluded from the dataset since it does not contain explicit guidelines or recommendations. However, Livingstone et al. [20] and Iftikhar et al. [14] both include Ghosh et al. [11] and the discussed topics in their list of recommendations. The same applies to papers presenting critical issues for parental control [26, 30] that lacked well-defined recommendations. This led to the final nine, which will be presented in-depth in the next section.

4 RESULTS

This section presents the final iteration of the in-depth literature review, displayed in Figure 2. These form the basis to establish the recommendations for future parental control in the next section.

P1 : *A Study of Parental Control Requirements for Smart Toys* [1]
P2 : *Security Requirements and Tests for Smart Toys* [6]
P3 : *Privacy requirements in toy computing* [28]
P4 : *Privacy Report Card for Parental Control Solutions* [22]
P5 : *A Vulnerability Assessment on the Parental Control Mobile Applications' Security: Status based on the OWASP Security Requirements* [4]
P6 : *User Interface Design Model For Parental Control Application On Mobile Smartphone Using User-Centered Design Method* [32]
P7 : *Designing Parental Monitoring and Control Technology: A Systematic Review* [14]
P8 : *Understanding of user needs and problems: A rapid evidence review of age assurance and parental controls* [20]
P9 : *The digital competence framework for primary and secondary schools in Europe* [13]

Figure 2: The final iteration in the literature review.

Smart toys. P1, P2, and P3 address requirements in the context of smart toys. P3 outlines six privacy requirements for smart toys and emphasizes the parents' need to identify or modify the collected data. In addition, they should be informed of data exchange with third parties, and if so restrict it. P2 further addresses information security issues and derives 16 security requirements for smart toys based on threat modeling. They highlight user authentication, file integrity, and encryption of the data collection. Lastly, P1 compiles both privacy and security, along with legal, implementation, and interoperability requirements of smart toy parental apps based on privacy regulations (e.g., GDPR, COPPA), parental control evaluation tools, and scientific papers. In total, 37 (19 functional and 18 non-functional) requirements were identified. The requirement is highly relevant for parental control solutions in terms of increased security, privacy, and usability.

Table 1: The total search results from the literature review, with the search timeline starting from Jan 2015-Mar 2022.

Web library / search words	"parental control" AND "security" AND "application"	"parental control" AND "privacy" AND "application"	"parent? mediation" AND "child?" AND "security"	"child?" AND "online risk?" AND "security"
ACM	99(5)	96(0)	4(0)	22(3)
IEEE Explore	8(0)	2(1)	2(2)	26(2)
Scopus	22(1)	13(0)	0	10(1)

Parental control applications. The next papers consider parental control applications residing within computers, mobiles, and external applications. P4 and P5 apply a technical context and discusses the lack of security and privacy controls. P4 analyzes various parental control applications and provides six privacy recommendations. The difference from the smart toys papers is the focus on restricting third-party development libraries to limit the data collection. Moreover, P5 applies the requirements from The Open Web Application Security Project (OWASP) named Mobile Application Security Verification Standard (OWASP-MASVS) [24], a set of security requirements for mobile applications, to determine the security of several mobile parental control apps, and propose technical solutions.

Usability of application. Three papers in the dataset address usability in parental control. P6 conducted interviews with parents and observations with children by applying a user-centered design method. They derive five usability requirements for parents and two for the children from the design method, such as an improved interface with information about apps in app stores, deciding which applications the children may download, and encouraging user manuals for the parents. P7 synthesized five design guidelines from a systematic literature review to improve the user design on parental control. They address challenges such as flexibility for different styles, ages, and contexts, education for children about online dangers, and the design contribution of children. Likewise, P8 explains an essential perspective on regulation, and supervision while respecting children's rights in age and maturity. Their results indicate the parents' need to be technically adequate since too much limitation on children results in frustration, and restricting access does not automatically implicate a reduction in online harm.

Digital Intelligence Framework. This topic differs from the rest of the dataset since it includes guidelines for topics within digital intelligence, and is not directly concerned with parental supervision. Nonetheless, the inclusion of learning digital skills contributes to developing future parental control beyond the traditional functionalities. P9 contains a compiled list of competencies that primary and secondary school children are expected to learn. The first set of ten requirements within "Digital citizenship" is the most relevant to attain through parental control. Safeguarding sensitive information, and encouraging digital well-being could increase children benefiting from online services in a healthy manner.

5 PARENTAL CONTROL RECOMMENDATIONS

This section unveils the most relevant recommendations from the collected literature, for the future development of mobile parental controls, highlighting increased security, privacy, and usability. Figure 3 provides an overview of the relevant recommendations synthesized from the collected literature.

Usability

R1 : Present templates, and provide recommendations for using the application.
R2 : Include the children and parents in the design and development process of the application.
R3 : Adapt according to the child's age and parenting styles.
R4 : Support for multiple platforms.

Security

R5 : Increase security awareness amongst children and parents through using parental control.
R6 : Follow security standards and procedures.

Privacy

R7 : Monitor the children's activity in a non-intrusive way.
R8 : It should be clear what the parents' consent to in terms of sharing privacy-sensitive information about their child.
R9 : Parents are granted access to the child's data and should be able to delete or restrict the data collected by the application.

Figure 3: Recommendations for parental control

The compiled list of recommendations in Figure 3 addresses crucial privacy, security, and usability challenges in mobile parental control. They advocate proper identity verification from parents, user authentication, and deleting Personal Identifiable Information (PII). Further, they discuss the need to increase security awareness among children and parents and sustain the child's personal life by increasing their digital intelligence. Privacy awareness is equally important, but in contrast, there has been considerable progress in that area already [27]. The adoption could increase if parents and children's feedback and participation contributed to the development process. Figure 4 presents the extracted recommendations according to their level of concreteness (system/technical level) vs. abstractness (design/non-technical level), where the latter requires a more holistic approach.

5.1 Usability recommendations

According to the literature found [1, 14], parents struggle to fully benefit from parental control applications. Providing the parents with pre-defined templates on rules, blocking/limiting the use of applications, and filters could benefit appropriate parental control use. These templates should be combined with other self-defined

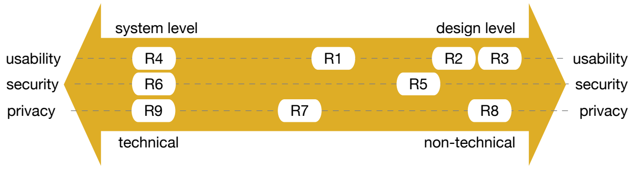

Figure 4: Relative positioning of the recommendations in terms of the level of abstraction and technical vs. non-technical.

rule sets to meet the various parenting styles. However, the choice of the rule set and blocking should be discussed with the children, which becomes more necessary as their age increases.

In addition, parents should be able to exchange experiences from benefiting the application could increase their knowledge and the usability of the application. For instance, enabling F&Q sections or discussion forums for parents creates new solutions to share with each other. Parents and children could provide suggestions for much-needed functionalities directly to the developing team. Children, in particular, could carry valuable suggestions as they age and mature. Hence, continuously improving parental control could increase the adoption of the application.

Parental control should accommodate different parental styles and ages [20]. Future solutions require upholding the inclusion of various online child-rearing practices. If not, they risk not being correctly adopted by users in other countries and cultures. For instance, the amount of monitoring may vary according to the society's digital maturity level, cultural differences, age, and parenting style. Respecting user diversity may be the key to persuading parents to use parental controls regarding learning digital independence and cybersecurity principles. Furthermore, children should be involved in such applications' design and development process to a greater extent. This might increase the parent-child communication, so the children are aware of being open about online issues arising. [14].

The same study [14] reported a lack of cross-platform tools, where one application could be applied on different digital platforms. Nowadays, parental control solutions might not be compatible if parents' and children's smart devices possess distinct operating systems. Lock-in mechanisms significantly contribute to procuring devices from the same digital ecosystem. Supporting multiple digital platforms with the same application might also increase parental control usage.

5.2 Security recommendations

To further increase the parents' knowledge and contribute to their children's digital education, the application should provide them with information regarding the importance of digital well-being, and cybersecurity knowledge [13, 26]. Parental controls should possess additional tips regarding lists of downloadable applications with age restrictions, and overall rights and online experiences. Children should also benefit from learning about security concepts (e.g., safe password practices, information sharing, and social media) so that they are more capable of using and assessing digital services themselves.

Since current solutions struggle to adhere to privacy and security controls [2, 4], considerable efforts are required for future solutions to meet the existing regulations (e.g., OWASP). Therefore, while R6 may be perceived as overlapping with general privacy and security needs, it is still necessary to include it as a minimum requirement. The application should generally authenticate parental users, and provide a complete overview of financial transactions and/or app downloads [6]. The parental device(s) and users should be verified to ensure misuse of the child's data from unknown devices by for instance applying e-mail confirmations, digitally signing the consent, and/or pre-authorized credit card [1, 6].

5.3 Privacy recommendations

Mobile parental control should possess some monitoring of the children's digital usage, due to inexperience, maturity, cultural differences, and parenting style. Nonetheless, it should not be too intrusive, by containing enough to observe overall trends and patterns in their digital habits, but not expose their privacy to the parents [14, 20, 32]. There should be an indicator displaying on the child's device so that they are aware of the monitoring [7]. Adolescents, teenagers, and sufficiently mature children should carry the possibility to decline monitoring [1]. By obscuring the information, the parents are induced to communicate directly with the child.

As previously mentioned, the efforts to adhere to existing regulations (e.g., COPPA, GDPR) must be intensified , as emphasized by R9. R8 highlights the importance of proper consent to monitor the child's smart device data and parents approving application downloads. Knowledge about the extent of their consent should be conveyed in an understandable manner, both to parents *and children* [7, 32]. Lastly, parents should be able to locate, inspect and delete all data of their children, and Personally Identifiable Information (PII) from the application [1].

5.4 Limitations

The timeline, keywords, and search items were identified using the problem statement, but due to the selection, there is a risk of excluding relevant literature. The risk could be further increased by only selecting a limited number of bibliographic databases. This risk was mitigated by performing an additional manual search on Google Scholar.

6 CONCLUSION AND FUTURE WORK

Children and adolescents are becoming the most avid digital users by participating in digital games, benefiting social media, and watching online content. This paper presents three privacy, two security, and four usability recommendations elicited from an in-depth literature review. According to the literature findings, parental control should improve security and privacy measures, clarify parental consent, support multiple platforms, and adapt to different parental styles, cultures, and ages. Follow-up, future work should incorporate papers without clear recommendations/guidelines in a systematic analysis with a broader time span, other web libraries (e.g., DBLA, Web of Science), and topics (e.g., within social sciences) to propose in-depth requirements based on literature regarding parental control. Our current work is conducting qualitative research on the users, which could provide relevant feedback to supplement the literature findings, along with how different age groups, cultural differences, and the meaning of consent affect parental control. Mobile parental control holds the potential to develop into a beneficial tool to enhance children's understanding of online risk, privacy, and security principles, and foster beneficial digital habits.

ACKNOWLEDGMENTS

This research was conducted as a part of a master's thesis in Communication Technology at the Norwegian University of Science and Technology submitted in June 2022 with co-student Herborg Kristiansen Hatlen. The authors thank the anonymous EICC 2023 reviewers for their insightful suggestions and comments.

REFERENCES

[1] Otavio De P. Albuquerque, Marcelo Fantinato, Marcelo M. Eler, Sarajane M. Peres, and Patrick C.K. Hung. 2020. A Study of Parental Control Requirements for Smart Toys. In *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 2020-October. Institute of Electrical and Electronics Engineers Inc., Toronto, ON, 2215–2220. https://doi.org/10.1109/SMC42975.2020.9282959

[2] Suzan Ali, Mounir Elgharabawy, Quentin Duchaussoy, Mohammad Mannan, and Amr Youssef. 2021. Parental Controls: Safer Internet Solutions or New Pitfalls? *IEEE Security and Privacy* (2021), 1–11. Issue ii. https://doi.org/10.1109/MSEC.2021.3076150

[3] Hamza H.M. Altarturi, Muntadher Saadoon, and Nor Badrul Anuar. 2020. Cyber parental control: A bibliometric study. *Children and Youth Services Review* 116 (9 2020). https://doi.org/10.1016/j.childyouth.2020.105134

[4] Eric B Blancaflor, Gerardine Anne J Anson, Angela Mae V Encinas, Kiel Cedrick T, Mark Anthony V Marin, and Stephany Lhaime G Zamora. 2021. A Vulnerability Assessment on the Parental Control Mobile Applications ' Security : Status based on the OWASP Security Requirements. In *Proceedings of the 11th Annual International Conference on Industrial Engineering and Operations Management.* IEOM Society International, Singapore, 6463–6472.

[5] Lorrie Faith Cranor, Adam L Durity, Abigail Marsh, and Blase Ur. 2014. Parents' and Teens' Perspectives on Privacy In a Technology-Filled World. In *Tenth Symposium On Usable Privacy and Security (SOUPS) 2014.* USENIX Association, Menlo Park, CA.

[6] Luciano Gonçalves de Carvalho and Marcelo Medeiros Eler. 2018. Security requirements and tests for smart toys. In *Enterprise Information Systems: 19th International Conference, ICEIS 2017, Porto, Portugal, April 26-29, 2017, Revised Selected Papers 19.* Springer, 291–312.

[7] Anirudh Ekambaranathan and Jun Zhao. 2021. Money makes the world go around: Identifying barriers to beter privacy in children's apps from developers' perspectives. In *Conference on Human Factors in Computing Systems - Proceedings.* Association for Computing Machinery, New York, NY, 1–15. https://doi.org/10.1145/3411764.3445599

[8] Álvaro Feal, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso, and Alessandra Gorla. 2020. Angel or Devil? A Privacy Study of Mobile Parental Control Apps. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (04 2020), 314–335. https://doi.org/10.2478/popets-2020-0029

[9] Federal Trade Commission. 2017. Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business. https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance. [Accessed 12. Nov. 2021].

[10] Walter Fuertes, Karina Quimbiulco, Fernando Galárraga, and José Luis García-Dorado. 2015. On the Development of Advanced Parental Control Tools. In *2015 1st International Conference on Software Security and Assurance (ICSSA).* IEEE, 1–6. https://doi.org/10.1109/ICSSA.2015.011

[11] Arup Kumar Ghosh, Karla Badillo-Urquiola, Mary Beth Rosson, Heng Xu, John M. Carroll, and Pamela J. Wisniewski. 2018. A Matter of Control or Safety? Examining Parental Use of Technical Monitoring Apps on Teens' Mobile Devices. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18).* Association for Computing Machinery, New York, NY, USA, 1–14.

[12] Arup Kumar Ghosh, Charles E. Hughes, and Pamela J. Wisniewski. 2020. Circle of Trust: A New Approach to Mobile Online Safety for Families. In *CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems.* Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376747

[13] Montse Guitert, Teresa Romeu, and Pablo Baztán. 2021. The digital competence framework for primary and secondary schools in Europe. *European Journal of Education* 56, 1 (2021), 133–149. https://doi.org/10.1111/ejed.12430

[14] Zainab Iftikhar, Qutaiba Rohan ul Haq, Osama Younus, Taha Sardar, Hammad Arif, Mobin Javed, and Suleman Shahid. 2021. Designing Parental Monitoring and Control Technology: A Systematic Review. In *Human-Computer Interaction – INTERACT 2021.* Springer Nature Switzerland AG, Bari, Italy, 676–700. https://doi.org/10.1007/978-3-030-85610-6_39

[15] Intersoft Consulting. 2018. General Data Protection Regulation (GDPR). https://gdpr-info.eu. [Accessed 12. Nov. 2021].

[16] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 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 (11 2017). Issue CSCW. https://doi.org/10.1145/3134699

[17] Ilaria Liccardi, Monica Bulger, Hal Abelson, Daniel J. Weitzner, and Wendy Mackay. 2014. Can apps play by the COPPA Rules?. In *2014 12th Annual Conference on Privacy, Security and Trust, PST 2014.* Institute of Electrical and Electronics Engineers Inc., 1–9.

[18] Sonia Livingstone, Leslie Haddon, Anke Görzig, and Kjartan Ólafsson. 2011. Technical report and user guide: The 2010 EU kids online survey. *LSE, London: EU Kids Online* (2011).

[19] Sonia Livingstone, Kjartan Ólafsson, Ellen J. Helsper, Francisco Lupiáñez-Villanueva, Giuseppe A. Veltri, and Frans Folkvord. 2017. Maximizing Opportunities and Minimizing Risks for Children Online: The Role of Digital Skills in Emerging Strategies of Parental Mediation. *J. Commun.* 67, 1 (2 2017), 82–105. https://doi.org/10.1111/jcom.12277

[20] Sonia Livingstone and Mariya Stoilova. 2021. *Understanding of user needs and problems : A rapid evidence review of age assurance and parental controls.* Technical Report September. London School of Economics and Political Science (LSE), London. 60 pages.

[21] Emmanouil Magkos, Eleni Kleisiari, Panagiotis Chanias, and Viktor Giannakouris-Salalidis. 2014. Parental control and children's internet safety: the good, the bad and the ugly. *6th International Conference on Information Law and Ethics (ICIL 2014)* (2014), 829–847.

[22] Mohammad Mannan, Amr Youssef, Suzan Ali, and Quentin Duchaussoy. 2019. *Privacy Report Card for Parental Control Solutions.* Technical Report. Concordia Institute for Information Systems Engineering (CIISE), Montreal.

[23] Marije Nouwen, Maarten Van Mechelen, and Bieke Zaman. 2015. A value sensitive design approach to parental software for young children. In *IDC '15: Proceedings of the 14th International Conference on Interaction Design and Children.* Association for Computing Machinery, New York, NY, USA, 363–366. https://doi.org/10.1145/2771839.2771917

[24] OWASP. 2020. OWASP Mobile Application Security Verification Standard. https://github.com/OWASP/owasp-masvs [Online; accessed 16. Feb. 2023].

[25] Aarathi Prasad, Ruben Ruiz, and Timothy Stablein. 2019. Understanding Parents' Concerns with Smart Device Usage in the Home. In *HCI for Cybersecurity, Privacy and Trust.* Springer, Cham, Switzerland, 176–190. https://doi.org/10.1007/978-3-030-22351-9_12

[26] Farzana Quayyum, Jonas Bueie, Daniela S. Cruzes, Letizia Jaccheri, and Juan Carlos Torrado Vidal. 2021. Understanding parents' perceptions of children's cybersecurity awareness in Norway. In *Conference on Information Technology for Social Good (GoodIT '21).* Association for Computing Machinery (ACM), 236–241. https://doi.org/10.1145/3462203.3475900

[27] Farzana Quayyum, Daniela S. Cruzes, and Letizia Jaccheri. 2021. Cybersecurity awareness for children: A systematic literature review. *Int. J. Child-Comput. Interact.* 30 (12 2021), 100343. https://doi.org/10.1016/j.ijcci.2021.100343

[28] Laura Rafferty, Marcelo Fantinato, and Patrick CK Hung. 2015. Privacy requirements in toy computing. *Mobile services for toy computing* (2015), 141–173.

[29] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman. 2018. Won't Somebody Think of the Children? Examining COPPA Compliance at Scale. *Proceedings on Privacy Enhancing Technologies* 2018 (2018), 63–83. Issue 3. https://doi.org/10.1515/popets-2018-0021

[30] Diane J. Schiano, Christine Burg, Anthony Nalan Smith, and Florencia Moore. 2016. Parenting digital youth: How now?. In *Conference on Human Factors in Computing Systems - Proceedings.* Association for Computing Machinery, 3181–3189.

[31] D. Smahel, H. Machackova, G. Mascheroni, L. Dedkova, E. Staksrud, K. Ólafsson, and U. Hasebrink. 2020. *EU Kids Online 2020: Survey results from 19 countries.* Technical Report. EU Kids Online.

[32] Syafrizal Wardhana, Mira Kania Sabariah, Veronikha Effendy, and Dana S Kusumo. 2017. User interface design model for parental control application on mobile smartphone using user centered design method. In *2017 5th International Conference on Information and Communication Technology (ICoIC7).* IEEE, Melaka, Malaysia, 1–6.

[33] Pamela Wisniewski, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2017. Parents just don't understand: Why teens don't talk to parents about their online risk experiences. In *Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW.* Association for Computing Machinery, 523–540. https://doi.org/10.1145/2998181.2998236