


Is My Child Safe Online? - On Requirements for Parental Control Tools in Apps used by Children

João Victor Assis  [Federal Rural University of Pernambuco | joao.ctassis@ufrpe.br]

George Valença   [Federal Rural University of Pernambuco | george.valenca@ufrpe.br]

 Computing Department, Federal Rural University of Pernambuco, Dom Manuel de Medeiros Street, Recife, PE, 52171-900, Brazil.

Received: 11 March 2024 • Accepted: 02 August 2024 • Published: 08 August 2024

Abstract: Following the Covid-19 pandemic, children have increased their use of mobile electronic devices to access the internet. Among the main applications used by children between 9 and 17 years old are the social and communication media platforms Instagram and TikTok. Consequently, they are more exposed to risky situations (e.g. objectionable content, sexual predators, cyberbullying, etc.). To address this scenario, we conducted a systematic mapping study and a snowballing process evaluating 33 primary studies to identify recommendations and general guidelines for parental control tools, which should be part of any social media app used by children. Based on this study, we derived 16 functional (FR) and 13 non-functional requirements (NFR) for IT companies to develop features that help caregivers and children promote online protection via assertive decisions and proper safeguards. We used those functional requirements as lenses of analysis of the two main social media software platforms largely used by children: Instagram and TikTok. Our findings revealed that TikTok's parental control features are more mature and present more options for supervising and restricting children's online activities than Instagram's. Therefore, this research expands knowledge about the features for parental control and raises the discussion around children's protection and welfare as relevant digital citizens.

Keywords: Parental Control, Children, Requirements, Apps, social media, Features

1 Introduction

After the Covid-19 pandemic, we observed an increase in the use of electronic devices by children, with the proliferation of connected gadgets such as smartphones and tablets in their routines (e.g. in classes, for online interaction with friends or simply for fun - playing games or watching their favorite vlogs). In Brazil, children are becoming familiar with digital technology at an increasingly young age, with a frequent use of the internet – The number of children who had their first access to the internet by the age of 6 increased by 10.5% between 2018 and 2022 [CGI.br, 2023].

The disparity in the use of mobile devices such as smartphones, tablets, and smart devices over other devices such as desktop computers causes a large use of mobile apps in a regular user's journey [CGI.br, 2023]. At the same time, one-third of users globally are children [UNICEF, 2019], which denotes their relevance for IT companies.

In 2022, 86% of Brazilian internet users between 9 and 17 years old already had a profile on at least one social media platform [CGI.br, 2023]. To ensure children's well-being, avoiding the excessive use of their data and situations that affect their online security, we must understand if their preferred apps provide parental control features. The top-3 social and communication media platforms apps used by Brazilian children aged 9 to 17 [CGI.br, 2023] is formed by TikTok, Instagram, and Facebook, each one implementing its own parental control features.

According to the Brazilian Society of Pediatrics (SBP), children's overexposure to electronic devices at an early age can trigger social, behavioral, sleep, and eating problems, as

well as increase anxiety and expose children to inappropriate content for their age group [Penina, 2017]. According to The Guardian, former employees of tech companies struggle with safety concerns over their children's use of social media¹. This context reinforces the need for proper knowledge about parental control tools, which represents an option for protecting children in the digital environment.

From the legal perspective, Brazilian Civil Rights Framework for the Internet (in Portuguese: Marco Civil da Internet, officially (Federal) Law No 12.965/2014) regulates the use of the Internet by defining ethical principles and guarantees for the digital environment to be a free and democratic space, with a focus on ensuring privacy and personal data protection [BRAZIL, 2014]. This legislation reinforces the prohibition of child advertising [BRAZIL, 1990b] and the total priority for the protection of children's rights by society, the state and companies [BRAZIL, 1988]. The Brazil's General Data Protection Law (in Portuguese: Lei Geral de Proteção de Dados Pessoais - LGPD, officially (Federal) Law No 13.709/2018) regulates the processing of children's personal data, establishing among others that their data must be processed in their best interest, and stating the age of consent for data collection as 13 years old [BRAZIL, 2018].

Internationally, there are two famous important data protection regulations. The Children's Online Privacy Protection Act (COPPA)² in the United States, regulates organiza-

¹The Guardian - January 2024. "Fundamentally against their safety": the social media insiders fearing for their kids" - Available on <http://tinyurl.com/4zz6hsyh>

²Children's Online Privacy Protection Act (COPPA). Available on: <http://tinyurl.com/3zwxvzpd>

tions that collect and use data from children under the age of 13. The European General Data Protection Regulation (GDPR)³ is a comprehensive data protection framework. It identifies children as a vulnerable group requiring special safeguards, particularly in the collection of personal information from those under 16 years old. Both regulate collection, storage and processing without parental consent of children's personal data under a certain defined age.

In another perspective, social media apps used by young users have age ratings. Highly relevant platforms like Instagram and TikTok, for example, require a minimum age of 13 for registration. However, immature age verification mechanisms enable underage youth to create profiles and start exploring these platforms [Pasquale *et al.*, 2022]. In addition, these platforms often expose children to advertising and inappropriate content such as pornography, drugs, violence and cyberbullying, or self-harm⁴.

Many parents are not familiar with technological tools, including those provided by apps used by their kids, which prevent children from getting proper guidance [Matos, 2021]. In addition, less than 10 percent of children on Instagram had enabled the parental supervision setting by the end of 2022⁵. Therefore, two problems emerge: (i) a lack of assertive communication for the protection of children in the digital environment, and (ii) excessive and unsupervised use of smartphones, the main vector of internet access for young people [CGI.br, 2023]. This scenario motivated us to explore the following research questions (RQ):

- RQ1 - What are the ideal requirements for parental control features in social media apps used by children?
- RQ2 - What are the key features for parental control offered by social media platforms?

To address RQ1, we identified the ideal requirements for parental control tools in the literature through a systematic mapping study that encompassed a snowballing process. Our analysis of 33 primary studies enabled the definition of 29 requirements, which we classified in 2 main categories: non-functional requirements and functional requirements (categorized into 4 dimensions). As an additional contribution, we addressed RQ2 by using the defined functional requirements to examine features for parental control provided by the two main social media platforms most commonly used by children from 9 to 17 years old: Instagram and TikTok [CGI.br, 2023]. The research steps were conducted by the first author under the supervision of the second author, an expert in the field of Human-Machine Interaction who reviewed each preliminary result (e.g. he strengthened the study by indicating papers to include in the mapping phase, during snowballing).

The rest of this paper is structured as follows. In Section 2, we present our conceptual background. Section 3 details

the methodology. Sections 4 and 5 present our contribution: (i) the list of requirements for parental control tools, and (ii) their application to examine two social media platforms, TikTok and Instagram. Finally, Section 6 describes the research's impact on academia and practice, together with threats to validity and future work.

2 Conceptual Background

2.1 Children's Protection Online

Internationally, the United Nations' Convention on the Rights of the Child (CRC) defines a **child** as any person up to 18 years of age [United Nations, 1989]. In Brazil, the Child and Adolescent Statute divides this period into two age groups, defining a child as up to 12 years old and an adolescent from 12 to 18 years old [BRAZIL, 1990a]. This research adopts the more general concept given by the CRC for generalization purposes, considering children up to 18 years old.

Pasquale *et al.* [2022] depicts the flaws and vulnerabilities of age verification in the top 10 social media platforms used by children in 2019 and 2020. As some of them do not even ask for age during registration, children find ways to bypass existing verification mechanisms. In addition, the work also highlights the limited number of alternative versions of some of these applications (e.g. YouTube Kids) created for children up to 13 years old, which reinforces the adoption of the standard versions by children and exposes them to objectionable content developed for adults.

In this scenario, **parental control tools** are technologies and functionalities for monitoring and/or limiting (e.g. decrease the time spent in apps as well as restricting what types of content they can interact with) children's access to software solutions such as games and social media [Nouwen *et al.* [2017]. Their main features include: (1) restricting usage time; (2) restricting content accessed by children (e.g. age-inappropriate content); (3) restricting activities, such as online purchases, social interactions with strangers, flagged websites access, and multiplayer entertainment activities; and (4) monitoring and tracking children's online activities (e.g. usage reports, access to history) [Zaman *et al.*, 2016].

Altarturi *et al.* [2020] introduces the notion of **cyber parental control** as parenting actions involving monitoring, controlling, and limiting children's activities on the internet, which involves parental *monitoring* (i.e. attention and tracking of children's activities), *mediation* (i.e. parents and children interaction with the media) and *control* (i.e. parents controlling children's activities and interactions). The authors discuss different forms of mediation, such as restrictive (e.g. limiting activities, time spent, and content seen) and evaluative (e.g. discussing internet risks and creating usage rules).

Tove Lafton and Holmarsdottir [2024] state that parental mediation involves not only regulation but also the dialogue between children and parents on their media use. These interactions can lead to agreements that benefit children's literacy and digital education, reducing risks and even promoting self-regulation (i.e. self-monitoring, impulse control, risk coping [Wisniewski *et al.*, 2017]).

³General Data Protection Regulation (GDPR). Available on: <http://tinyurl.com/4r6s6ej6>

⁴The Washington Post - February 2024. "These are the parents who stared down Mark Zuckerberg: They believe social media helped harm or kill their kids, and they're asking for regulation". Available on: <http://tinyurl.com/36drn4ew>

⁵The Washington Post - January 2024. "Meta says its parental controls protect kids. But hardly anyone uses them". Available on: <http://tinyurl.com/bdzcrxeb>

2.2 Related Work

Nouwen *et al.* [2017] describes parental control approaches to mediate children and caregivers' discussions about social media, based on collaboration and mutual learning. This work reinforces the need for improvement in parental control tools due to generational conflicts and a lack of digital literacy. Hence, it proposed co-creation sessions for improving such interaction (i.e. designing tools to assist parents in children's digital protection and/or education).

The study in de Paula Albuquerque *et al.* [2022] continues the work from Fantinato *et al.* [2017] by proposing a reference solution for parental control tools in Smart Toys. This work defined and empirically evaluated requirements to develop parental control tools for smart toys. It also proposed a conceptual model of features and a prototype of the tool serving as proof of concept. Although this work focuses on smart toys, we considered it as one source to extract requirements for parental control tools, abstracting functionalities that could be embedded in social media applications.

Mariya Stoilova and Livingstone [2024] conducted a rapid evidence review to investigate the contexts and outcomes associated with the use of parental control tools for child protection. The study identified which families use parental controls, why they use them, and the consequences of their use, whether positive, negative, limiting, or neutral. The investigation emphasized factors external to the technology (e.g., the age of parents and children, digital competencies, parental involvement, and motivation) in mitigating online risks. It examined the effectiveness of parental control tools without delving deeply into their functionalities or analyzing any specific tools available in the market.

The report from Smirnova *et al.* [2021] aimed to shed light on the effectiveness of age assurance mechanisms, barriers to accessing age-restricted content, children's strategies to bypass age verification systems, and potential risks to children's safety and privacy. The report based on empirical evidence to include insights for policymaking and highlight the limitations of existing age assurance measures.

In other perspective, the article from Ghosh *et al.* [2020] developed an Android app (i.e. Circle of trust) that incorporated design patterns commonly found in commercially available parental control apps. The report aimed to address the limitations of existing parental control tools and provide a more balanced and ethical solution to support parents and teens in managing online risks. Our work distinguishes from theirs in that we have formalized requirements for parental control tools and conducted an inspection of two applications based on these criteria. In contrast, their study compared the Circle of Trust app with traditional parental control applications involving 17 parent-child pairs.

Albuquerque *et al.* [2023] also explores the risks brought by social media platforms to children (in this case, those who are content producers) from the perspective of deceptive design patterns. However, the authors do not present requirements or best practices for children's protection in this scenario. Their contribution is a set of prototypes as suggestions to change platforms' features. In a similar way, Serra *et al.* [2021] explores the automatic detection of sensitive media in messaging apps. Instead of promoting what they consider

to be "invasive parental interventions", the study presents a different approach: self-monitoring control to video content in messaging apps to preserve a teenager's privacy.

We observed the literature on the topic commonly explores specific parental control applications, presenting features and requirements, or developing an app for this purpose. Considering this scope, in our work, we gather the main features of parental control tools within social media apps.

3 Research Method

The present study follows the qualitative research paradigm, seeking and analyzing academic papers through a mapping study to identify requirements for parental control tools in social media platforms, and then analyzing those tools in light of the requirements gathered. In Figure 1, we present the research phases with their respective activities (from 1.1 to 2.3), which we describe in the subsequent sections.

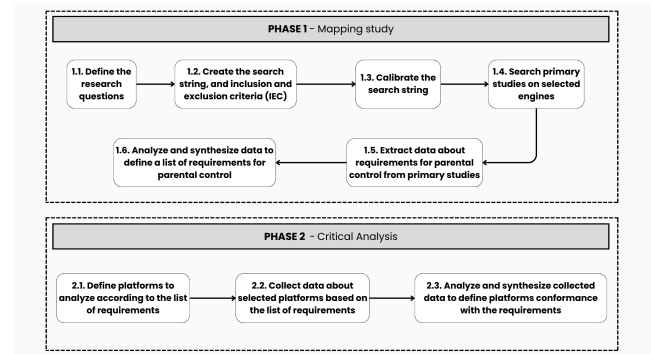


Figure 1. Research phases

3.1 Systematic Mapping Study

The first phase of this study consisted of a mapping study on parental control features. To address the first research question (RQ1), we performed a comprehensive literature review from March 2023 to January 2024. We aimed to identify the perspective of the literature regarding the optimal features for child protection on social media applications. Additionally, this study provided us with the main studies in this field. This phase comprised six steps related to the search process (also embracing a snowballing method) as well as data extraction, analysis and synthesis.

To **define the research questions (1.1)**, we performed an initial literature review on ACM Digital Library, IEEEExplore and Science Direct using terms such as "parental control", "age verification", and "social media and children". This activity provided us with an overview of the topic, revealing the main contributions in literature (e.g. guidelines, tools and previous literature reviews). Then, we **created a preliminary search string**, and formulated the **inclusion and exclusion criteria (IEC) (1.2)** (Table 1).

To **calibrate the search string (1.3)**, we analyzed the relevance and completeness of results on parental control. The final search string became:

Table 1. Inclusion and Exclusion Criteria

ID	Description
IC1	The study must be a scientific work (e.g. articles, theses, and dissertations).
IC2	The study must be in English.
IC3	The study was published between 2018 and 2023.
IC4	The study directly or indirectly focuses on features, requirements and/or recommendations for online parental control.
EC1	The study does not cover the topic of this research.
EC2	When there is more than one report from the same study, we considered the most complete version.

(parental OR parents OR caregiver) AND (control OR monitoring OR monitor OR controlling OR configure OR configuring) AND (digital OR tool OR mobile OR app OR platform OR Youtube OR TikTok OR Instagram OR Facebook).

We performed the **search process (1.4)** on four search engines: Google Scholar, IEEEExplore, Wiley Interscience, and ACM Digital Library using the previous search string. We highlight that, given the wide set of results provided by Google Scholar as a more general engine, we considered the initial 17 pages, with 170 articles analyzed.

Our timeframe, from 2018-2023, reflects the establishment of GDPR in Europe as well as the approval of LGPD (the Brazilian version of the European data protection law). Both laws raised the discussion about child protection on the internet and caused platforms to implement measures for children's security. For instance, in 2019, TikTok initiated the implementation of child protection features, expanding its filters to cater to different age groups [TikTok, 2019]. In 2020, TikTok introduced Family Pairing, a parental monitoring and control tool [TikTok, 2020]. Fast forward two years, in 2022, Instagram, renowned for its continuous efforts in enhancing security and privacy, unveiled the Family Center and Parental Supervision Tools [Meta, f].

The detailed process of selection of papers is presented in Figure 2. We obtained a list of 199 papers, which we filtered according to initial inclusion and exclusion criteria (i.e. paper's title, abstract, keywords, publication language, and year of publication). Based on their introduction, we could refine our perception about the relevance of each work, including those within our scope, and removing others that were less complete reports of the same study. After this, the results and discussion sections from the articles were read and analyzed to generate a total of 12 papers. Finally, via a snowballing process (backward and forward searches), we enriched the set of mapped studies, selecting those that directly or indirectly brought arguments about features, requirements, or recommendations for parental control. Then, we excluded duplicated and gray literature documents and included an expert referral (by the second author of this study) of a newly published article related to our research. Our initial set of primary studies involved 35 papers.

For **data extraction**, we detailed the article dataset (title, publication, year, country) into a systematic mapping spreadsheet (available in: [Systematic mapping](#)). To **extract relevant data (1.5)** from papers, we fully read each one to filter

and remove those that (i) neither exposed ideas about features, requirements or recommendations for parental control (EC1) nor (ii) provided a complete view of the research (i.e. acted as preliminary versions of other studies) (EC2). Hence, we excluded 2 articles, resulting in the final list of 33 studies to extract excerpts mentioning clear features or parental and children's needs in terms of protection online. These excerpts were structured in a requirements' extraction breakdown sheet (it can be accessed [here](#)) for further analysis, with the final requirements detailed in the "Data Extraction - Requirements" page.

When **analyzing the data (1.6)**, we extracted excerpts from primary studies, interpreted them, combining similar recommendations, requirements or restrictions. Then we defined titles or general statements, and synthesised descriptions to generate a requirement. For example, monitoring features such as monitoring screen-time, messages, usage reports overview, and financial requests were grouped and described in a single requirement. Then, we filtered the ones that could be or already were presented as tools in social media apps, resulting in the final requirement list.

We used the requirements ontology proposed by [Alrumaih *et al.*, 2020] to classify the non-functional requirements extracted as Usability, Efficiency, Security, Dependability, Regulatory, Ethical, Legislative, Environmental, Operational, or Development. We also generated four thematic dimensions to classify the functional requirements, considering our interpretation of the complete set: *Children's Safety*, *Platform-Parent-Child's Dialogue*, *Parent-Children's Privacy*, and *Restriction and Monitoring*.

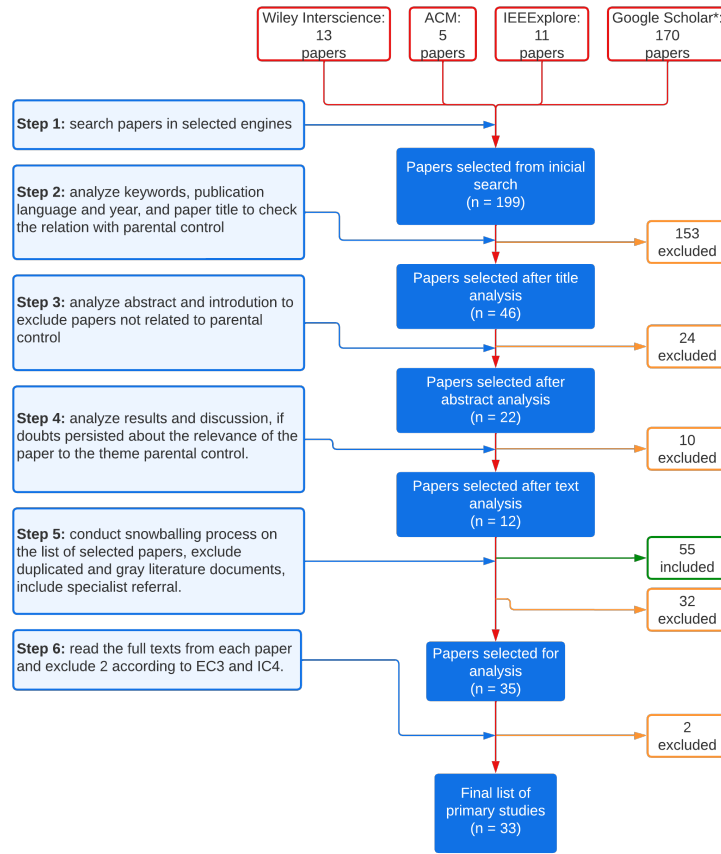
We highlight that demographic results of our mapping study, including temporal distribution of the papers and main contributors, are in a separate file, which is available at the following link: [Demographic results](#).

3.2 Social Media Platforms - Critical Analysis

In the second phase of this study, we examined two social media platforms in terms of their parental control features through an ad hoc inspection. The user interfaces from Meta's Family Center on Instagram and TikTok's Family Pairing were analyzed according to the set of functional requirements defined in the previous phase. We installed both applications and assessed their parental control features with the help of the documentation provided.

Initially, to **define the platforms (2.1)** to analyze, we considered that Instagram and TikTok figure as the social media apps most used by children from 9 to 17 years in Brazil, respectively, according to CGI.br [2023]. Hence, we selected these platforms due to their high popularity in this age group, accessible documentation and the possibility of instant communication through direct messages, which poses an additional danger for the child.

Then we **collected data about selected platforms (2.2)** based on the list of functional requirements, which focus on platforms' available parental control features. The functional requirements were listed in a spreadsheet, where we included information after examining the available documentation and performing an app analysis to check the conformance of features with the set of requirements.



*Google Scholar search was restricted to the timeframe of five years (2018 to 2023)

Figure 2. Search Process

The Instagram documentation was formed by its Tips for Parents section from the Help Center [Meta, d], and Family Center tools for Instagram [Meta, a], where guides and tips are available. When analyzing TikTok documentation, the selected materials were its Guardian’s Guide [TikTok, a], Children’s Privacy Policy [TikTok, c], Safety and privacy controls [TikTok, d], and Privacy and Security on TikTok [TikTok, b] pages. Finally, we **analyzed and synthesized (2.3)** collected data to both platform’s conformance with the set of functional requirements for parental control.

4 Results

The analysis of the 33 studies generated a set of 29 requirements, with 16 functional requirements (FR) (cf. Figure 3) and 13 non-functional requirements (NFR). We organized the FRs in four dimensions, which we explain in the following paragraphs: *Children’s Safety*, *Platform-Parent-Child’s Dialogue*, *Parent-Children’s Privacy*, and *Restriction and Monitoring*. When we mention the term parents we are also encompassing ”guardians” and/or ”caregivers”.

Children’s Safety requirements aim to protect children through digital education, live help functions, and assistance in using available tools. Hence, FR1-FR5 represents features to keep children safe online on social media. The tool should **allow children and parents to report inappropriate content** (FR1 - S20, 29 and S31) while using the app, also it

should **allow children to ask for help** (FR2 - S12 and S20) where the child can indicate a need for help with a certain content seen, for parents to review and dialogue later with them. To prevent children from coming in contact with objectionable content, the tool should **automatically detect and warn about risky content** (FR3 - S20 and S31). Besides, for parents to understand the tools and configure them more easily, the platform should **provide features to help using the tool** (FR4 - S1, S13, S14, S15 and S17) as well as providing ways to **raise children and parents’ awareness about online security** (FR5 - S1, S7, S8, S9, S12, S15, S17, S19 and S23).

Platform-Parent-Child’s Dialogue relates to the platform being able to listen to those who use it to evolve their tools and provide effective solutions for parent-children’s needs. For that, the platform should **provide communication channels to promote the discussion among parents, children, and the platform** (FR6 - S1 and S19). It should also **provide features and guidance materials to raise parents-children dialogue** (FR7 - S20), reinforcing the importance for the parents to dialogue with the children to help them learn how to use social media safely.

Restriction and monitoring requirements provide ways to **allow parents to monitor children’s activities** (FR8 - S1, S2, S4, S5, S8, S11, S12, S15, S17, S18, S19, S20, S22, S23, S28, S30, S31, S32 and S33), knowing what their teens are accessing online. The tool should also include features to **enable children’s self-monitoring and regulation** (FR9 -

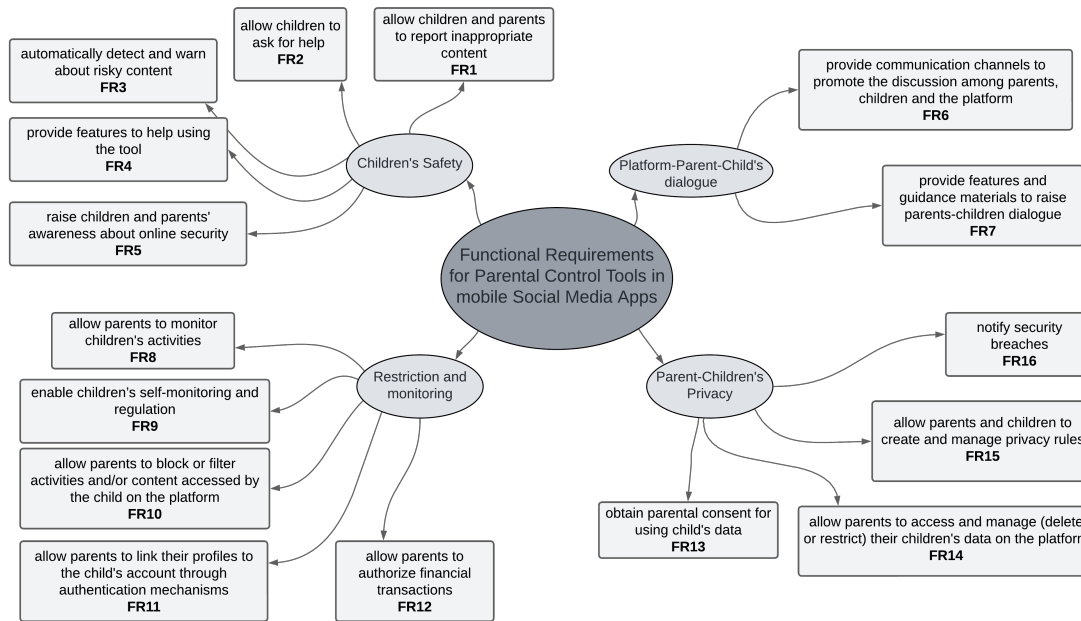


Figure 3. Functional Requirements for Parental Control Tools.

S8, S11, S19, S20, and S27), where they can be aware of their own activities and of how their caregivers are monitoring them. The tool should **allow parents to block or filter activities and/or content accessed by the child on the platform** (FR10 - S2, S3, S5, S8, S12, S18, S19, S20, S21, S22, S24, S25, S26, S27, S28, S29, S30, S31 and S33), setting rules that help them configure security and time usage settings for their children. For setting those features, it is necessary to **allow parents to link their profiles to the child's account through authentication mechanisms** (FR11 - S1, S16, S17, S20, S23, and S33), where the tool can give permissions for the parent's account to monitor and restrict multiple linked accounts for each teen in the family. Finally, the tool should be able to **allow parents to authorize financial transactions** (FR12 - S17) requested by teens for in-app purchases (when available).

The requirements for *Parent-Child Privacy* include features that enable a child or parent to control the stored and shared data. To create a child's account, companies should **obtain parental consent for using child's data** (FR13 - S15, S16, S17, S29, and S33). Besides, it should **allow parents to access, delete, or restrict their children's data on the platform** (FR14 - S1, S7, S9, S15, S16 and S17). Hence, parents must not only have access to these controls, but they also need to identify and manage them in an easy and intuitive way. Finally, companies should **allow parents and children to create and manage privacy rules** (FR15 - S15, S17, and S23) and **notify security breaches** (FR16 - S17) for parents to be informed about any data leaks.

Alrumaih *et al.* [2020] presents an ontology for Requirements Engineering, whose second level was used here for classifying **non-functional** requirements due to its sufficient degree of granularity. The authors classify such requirements as *Ethical*, *Legislative*, *Operational*, *Regulatory* (cf. Figure 4), *Security* and *Usability* (cf. Figure 5). In the following paragraphs, we describe the classes of non-functional requirements used to classify our requirements. It is possible

to obtain a wider set of details for such ontology by accessing the paper, which offers a description of all classes.

Ethical requirements define the constraints for the system to be acceptable to children's and parent's use, and it includes **monitor the children's activity in a non-intrusive way** (NFR1 - S1, S7, S8, S19, S20, and S27), except in cases of high-risk, or warning the child in advance. For the system to operate by laws defined for the online protection of children and their data, *legislative* requirements state the tool must **follow regulations and security standards and procedures** (NFR2 - S1, S7, S9, and S17). Privacy protection rules also define that **platforms should not allow third-party services to collect children's data** (NFR3 - S9).

The tool's *operational* constraints propose platforms to **consider data minimization and outgoing content blocking** (NFR4 - S7, S16 and S30), protecting children's data from being unnecessarily withheld, leaked, or misused. The tool must also **monitor and limit database growth** (NFR5 - S16). As the analyzed platforms are mobile social media apps, the tool must **require digital certificate for mobile services** (NFR6 - S16 and S17) as a *regulatory* requirement.

Security requirements state platforms must **maintain application settings every time parents or children use it** (NFR7 - S16 and S17). Besides, the tool must **encrypt personal information** (NFR8 - S16 and S17) shared with other apps or services, **restrict access to essential files on the phone** (NFR9 - S16), and **ensure accuracy of personal information** (NFR10 - S16) as necessary.

Finally, *Usability* requirements aim to improve parent's satisfaction using the platform, which should **provide support for multiple platforms** (NFR11 - S1, S3, and S17), and **provide parents with flexible and varied functionalities for parental control** (NFR12 - S1, S4, S7, S19, S20, S23 and S27) using varied parameters (e.g. child's age, parenting preferences, etc.). Hence, the tools must **address parents' needs** (NFR13 - S7, S17, S19, and S27), being easy to configure and use according to their capabilities and needs.

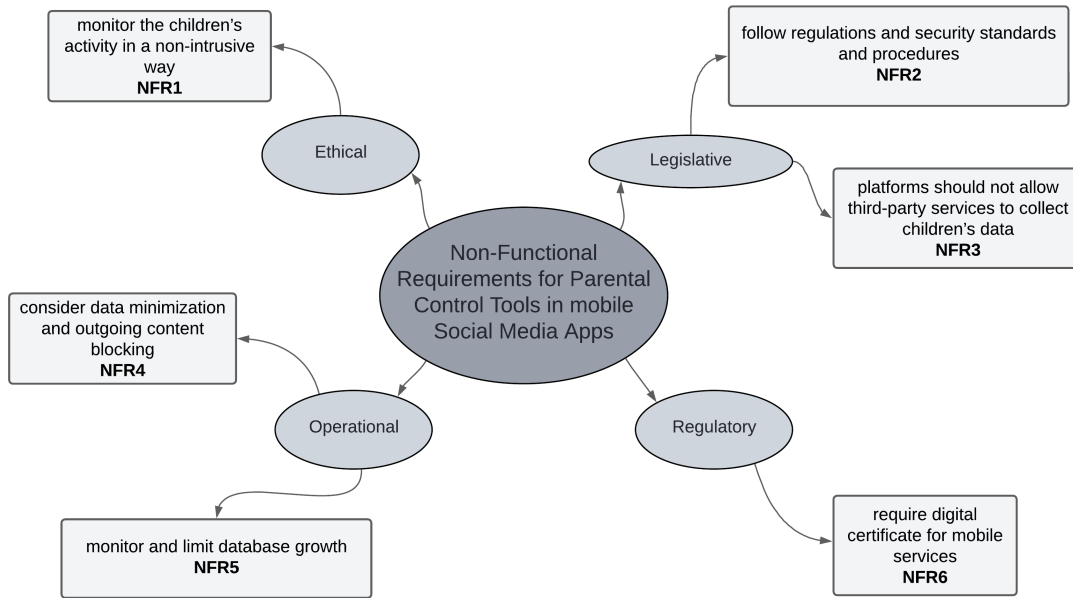


Figure 4. Non-Functional Requirements for Parental Control Tools (1-6).

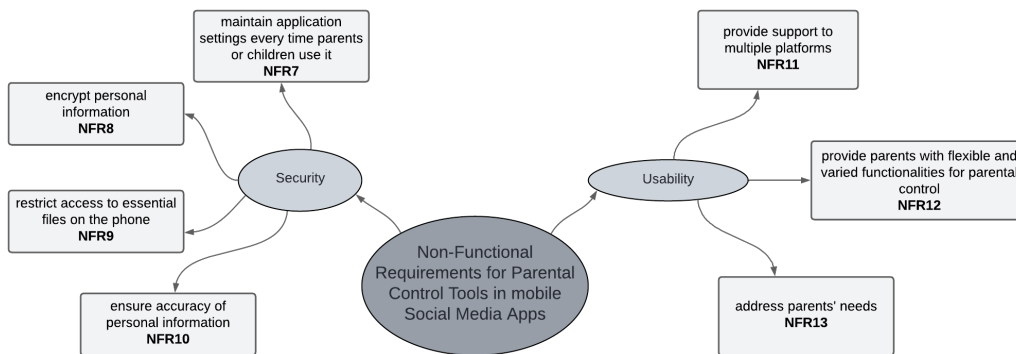


Figure 5. Non-Functional Requirements for Parental Control Tools (7-13).

5 A Case Study of Instagram and TikTok

In this section, we analyze our results by applying the final list of parental control requirements to assess two social media platforms. Hence, our discussion has two main outcomes: (i) exemplifying the use of the requirements and (ii) revealing the compliance of the selected platforms with the set of requirements for parental control (labeled as *full or partial compliance*, when the platform presents the functionality partially or completely meeting the requirement, *noncompliance*, when the platform does not present the functionality in its application or documentation, and *no substantial evidence of compliance*, when there is no sufficient evidence that could imply a compliance or noncompliance situation).

Figure 6 shows the requirements and the applications' compliance with the general descriptions of them, grouping partially and fully compliance into compliance. The detailed inspection compliance table is available in the following link: [Platforms' Compliance](#).

5.1 Instagram's Parental Control Tools

We found evidence that Instagram *fully or partially complies* with 11 of the 16 FRs raised, and *does not comply* with 3 FRs. Moreover, we did not have enough evidence to define compliance or noncompliance with 2 requirements (both from the *parent-children's Privacy* category), as shown in Figure 6. Meta cites privacy and security as pillars in building Instagram. In response to external pressure, the company states the efforts to make Instagram simpler for parents to oversee their teens' online lives [Meta, b]. Thereby, Meta's Family Center is focused on supervision, with few restriction options (FR10) for the parents to set up their children's accounts remotely (i.e. without having to use their child's phone). Instead, only the child can configure their privacy and restrictions, leaving the parent only to supervise.

Given the tool's nature, Meta provides content to increase security and privacy awareness among parents and children (FR5) encouraging dialogue and suggesting topics of conversation (cf. Figure 7) (FR7), while providing help centers, online content to help parents and children use it, and configures the children's account with pre-defined recommended privacy settings (cf. Figure 8) (FR4).

Instagram	Functional Requirement	TikTok
✓	FR1 - allow children and parents to report inappropriate content	✓
✗	FR2 - allow children to ask for help	✗
✓	FR3 - automatically detect and warn about risky content	✓
✓	FR4 - provide features to help using the tool	✓
✓	FR5 - raise children and parents' awareness about online security	✓
✓	FR6 - involve children and parents in the design and development process of the platform	✓
✓	FR7 - encourage dialogue between parents and children	✓
✓	FR8 - allow parents to monitor children's activities	✓
✓	FR9 - enable children's self-monitoring and regulation	✓
✓	FR10 - allow parents to block or filter activities and/or content accessed by the child on the platform	✓
✓	FR11 - allow parents to link their profiles to the child's account through authentication mechanisms	✓
✗	FR12 - allow parents to authorize financial transactions	✗
✗	FR13 - obtain parental consent for using child's data	✗
▬	FR14 - allow parents to access and manage (delete or restrict) their children's data on the platform	✓
✓	FR15 - allow parents and children to create and manage privacy rules	✓
▬	FR16 - notify security breaches	▬

Figure 6. Platforms' compliance to requirements. Full or partial compliance to the requirement is represented by the green check mark symbol, while noncompliance is represented by an red 'X' and no substantial evidence of compliance by a yellow horizontal bar.

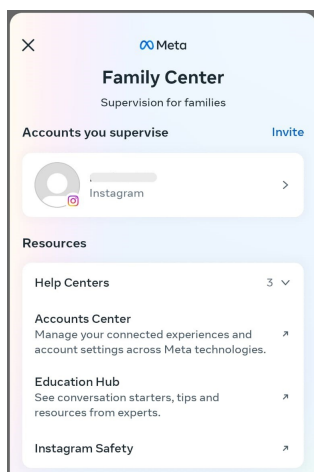


Figure 7. Some Instagram's resources for family in parent's phone (Feb. 2024)

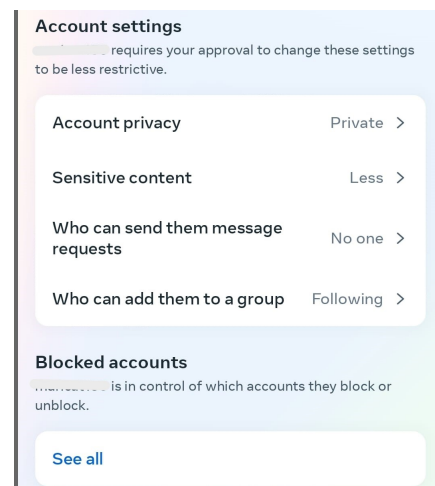


Figure 8. Some Instagram's supervision options in parent's phone (Feb. 2024)

Instagram doesn't offer functions for parents to authorize financial transactions through the app (FR12), even though it has a shopping feature and an in-app payment method (only available in the US, currently) [Meta, e]. Moreover, in Instagram's documentation, Meta states it grounds their development in research, direct feedback from parents, teens, experts, UN children's rights principles and global regulation

to build their safety and privacy options [Meta, b] (FR6).

Parents and teens in their own accounts must agree to set up supervision on the teen's account (FR11) as parents can supervise multiple teenagers. However, formally, teenagers aged 13 and over can create an account without needing parental consent (FR13), while children under the age of 13 cannot create an account. We must highlight that the In-

Instagram’s loose age verification mechanism has been scrutinized by State, federal legislators and caregivers in general as users can still misrepresent their birth dates when setting up an account, causing Meta to start introducing AI in this procedure (users will soon need to send a video selfie for Meta to estimate their age ⁶).

Instagram also does not state about parents accessing and controlling children’s data (FR14), even though they let the supervised account’s user (i.e. the child) locate, inspect, restrict and delete their own data from the platform in the account options [Meta, c].

Family center lets parents monitor their child’s activities (FR8) by seeing followers, following lists, time spent on the app and privacy options defined by the teenager; and receiving insights about reports filled by their teens of inappropriate content, user, or message, if they choose to share with the parents (FR1). Instagram does not have a button to ask parents for help on a specific topic or start a debate through the app (FR2), causing teens to seek out parents to report the content as inappropriate personally.

Therefore, Instagram provides parents with little control over teens’ choices for privacy and content. Instead, it provides information for teens’ self-monitoring and regulating, alerts the child about what information is being monitored (cf. Figure 9) (FR9), and encourages dialogue for setting those options for protecting them online. Instagram already sets default privacy and security settings based on the child’s age, filtering sensitive content (FR3). The role of parents in this regard is to approve or deny changes that their child wants to make in these settings (FR15) and talk about online security. In addition, parents can monitor and manage the time spent by their children using the app (cf. Figure 10) (FR8).

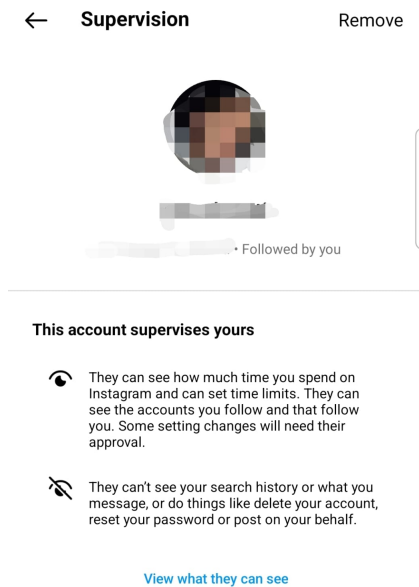


Figure 9. Instagram’s supervision message in child’s phone (Feb. 2024)

Finally, Instagram’s documentation does not mention how security breaches are treated (FR16 - e.g. strange behavior

⁶The Washington Post - June 2023. “Instagram rolls out age verification, but not to keep children off app”. Available on <http://tinyurl.com/5n8wtm3u>

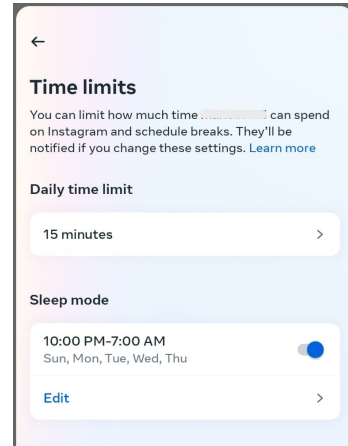


Figure 10. Instagram’s time limit options in parent’s phone (Feb. 2024)

from the child’s account, leakage of the child’s data, etc.). We highlight that, at any time, teens can remove the supervision, when the app will notify parents and provide 24 hours for the child to reconsider such configuration.

By offering limited control options and focusing on supervising children’s activities on the platform, Instagram requires parents to have a deeper understanding of potential online threats, smartphone proficiency, and security best practices to protect their children. The emphasis on supervision may be insufficient given the complexity of online interactions, reinforcing the importance of a more comprehensive approach that promotes not only surveillance but also easy controls for parents, and ongoing digital education to ensure the safety and well-being of children in the digital environment. In addition, limited transparency regarding data access and correction requests underscores the need for Instagram to enhance its parental control features.

5.2 TikTok’s Parental Control Tools

Our analysis gathered evidence that TikTok *fully or partially complies* with 12 of the FRs raised, and *does not comply* with 3 FRs. We did not have enough evidence to define compliance or noncompliance with 1 requirement (from the *parent-children’s Privacy* category).

Similarly to Instagram, TikTok suffers external pressure to provide a safe environment to children while using the app. It has a report option where the child can indicate inappropriate content, message, or user (FR1), but it does not provide an option for the children to indicate to parents when they need help on a specific topic or want to inform parents about something critical they saw online while using the app (FR2).

TikTok provides users with a help center formed by guardian guides [TikTok, a] that supports users to explore the tool (FR4), along with content to help parents and children learn about online security (FR5) and promote debate about some proposed topics (FR7). They state on their websites that feedback from parents and children is used to help improve their solutions and create more protection for children and parents online (FR6).

TikTok’s parental control tool is called *Family Pairing*, which enables parents to link their accounts to one or more teens (FR11) to monitor and manage children’s activities in the app. While TikTok filters risky content, it is also possible

for parents to set a restricted mode that reduces and notifies inappropriate or sensitive content (cf. Figure 11) (FR3).

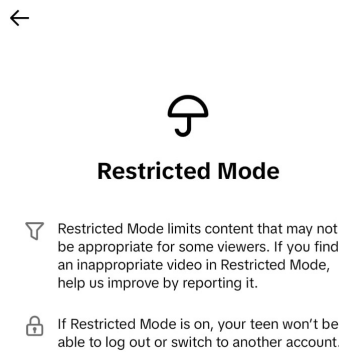


Figure 11. Tiktok’s restricted mode in parent’s phone (Feb. 2024)

A parent’s account can define (i) if the teen’s account is private and if TikTok can suggest the teen’s account to others, (ii) who can send direct messages to the teen, (iii) who can see the teen’s liked videos, and (iv) who can comment on the teen’s videos (cf. Figure 12) (FR8). Teens’ accounts have limited privacy options with mostly age-based predefined rules that can only be modified by the parents to more restrict options (FR15). Besides, parents and children can set content preferences (e.g. restricted mode, a content filter by keywords, disable comments, disable the search function for contents, etc) in addition to being able to limit the time the child spends on the application and determine times when it is not possible to use it (cf. Figure 13) (FR10). Children can also view all the information their parents are monitoring and the rules set by them (FR9), as shown in Figure 14.

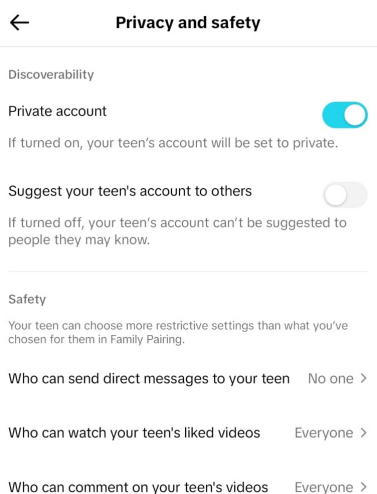


Figure 12. Tiktok’s privacy options in parent’s phone (Feb. 2024)

The platform does not have any functions regarding parents authorizing financial transactions through the app (FR12), even though it has a shopping function and an in-app payment method (currently unavailable in Brazil) [TikTok, e]. Besides, teenagers aged 13 and over can create an account without needing parental consent (FR13). Unlike Instagram, Tiktok explicitly states that the parent may submit a request to know, access, delete, or correct their child’s

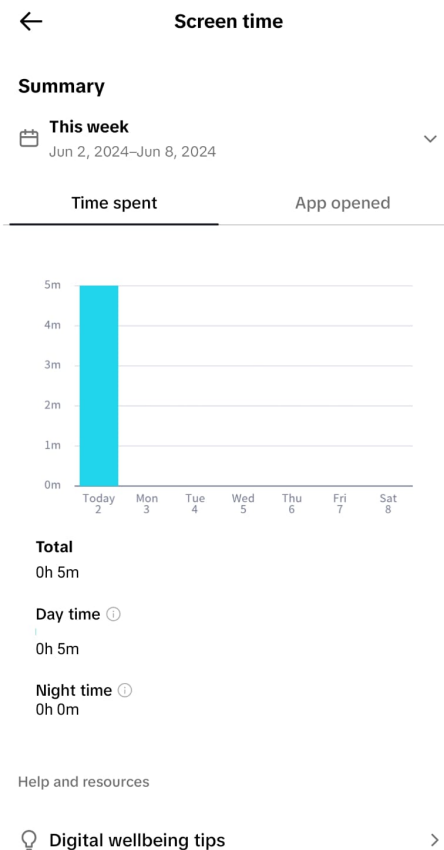


Figure 13. Tiktok’s screen time options in parent’s phone (Feb. 2024)

data collected [TikTok, c] (FR14). Lastly, we did not find any evidence that TikTok notifies parents in cases of security breaches (FR16). We highlight that at any time, the teen can remove the supervision, and then the app notifies the parent and gives 48h for the child to reconsider.

TikTok presents a solid parental control tool, with a variety of resources for caregivers to supervise the use of this social media platform by children over 13 years old. It also provides discussion topics and tips. The evolution of the *Family Pairing* tool could involve options to acquire and guarantee actual parental consent even when creating an account for a child. Moreover, some information about how children’s data are collected, used and shared should be easier to find.

6 Conclusion

6.1 Contribution for Research and Practice

This systematic mapping study on parental control tools in social media platforms used by children sheds light on the critical need for robust measures to ensure children’s online safety. By examining the requirements for parental control tools and conducting an analysis of the most popular social media platforms among children between 9 and 17 years old (i.e. Instagram and TikTok), it is evident that there is a pressing demand for enhanced features that cater to the specific needs of young users and parents.

Our findings revealed TikTok’s Family Link focuses on

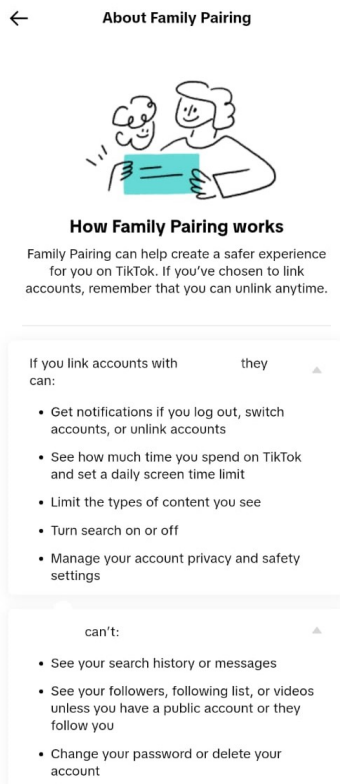


Figure 14. TikTok's family pairing message in child's phone (Feb. 2024)

Parental control features, where parents can restrict children's online activities. While Instagram presents a solid platform for parents to supervise children's activities online. Both platforms totally or partially comply with requirements from *Platform-Parent-Child's dialogue* category encouraging dialogue and considering parent-children opinions while developing these features. However, they still struggle to comply with *Parent-Children's Privacy* requirements, neglecting at least 2 requirements, and providing little information about some privacy concerns in parental control.

A challenge in the requirements development process was specifying requirements that were not originally intended for social media platforms. This challenge extended to the platform analysis, as some requirements pertained to functions that were not yet available on these platforms. Despite that, it was feasible to use the requirements to analyze the platforms' tools from the perspective of potential improvements and additions to enhance their comprehensiveness. Since most of these requirements are partially or fully implemented on the platforms, it bolstered our confidence in the results derived from extracting requirements from the literature.

We believe our findings are valuable for both academia and industry. By mapping parental control requirements and highlighting areas for improvement in social media platforms, we contribute to the ongoing dialogue on children's safety and education in the digital environment. These results underscore the importance of continuous evaluation and evolution of parental control tools on popular apps to better protect young users from potential risks and vulnerabilities in the digital space. We clarified the concept of parental control tools, and described the main parental control functionalities for children's safety in their preferred apps.

Moving forward, IT companies and policymakers must

collaborate in developing comprehensive parental control tools that prioritize children's safety and privacy. The alignment with international standards can provide more mature features and create a safer online environment for young users. This study serves as a possible catalyst for future research and innovation in the field of online child protection, emphasizing the shared responsibility of all stakeholders in safeguarding the well-being of our digital natives.

6.2 Threats to Validity

Even though we had systematically structured our work (e.g. using search string, performing a forward and backward search, extraction spreadsheet, etc.), our search procedure may have overlooked relevant articles, which is a threat to *internal validity*. To address this potential threat, we performed forward and backward searches and relied on expert referral, adding important studies (e.g. outside of our search time frame from 2018 to 2023).

To raise *construct validity*, we had one researcher mapping the data in the papers and another one validating the resultant selection and interpretation. These steps were critical since we were dealing with subjective evidence, such as non-functional requirements or how a given requirements was implemented by a company/platform. The use of an ad hoc inspection instead of a guided method to analyze the platforms also poses a threat as it limits to the author's perspective.

A potential threat to in terms of *conclusion validity* was restricting our analysis to the functional requirements. This was a research design decision considering our lack of access to relevant and sufficient data about non-functional requirements. For instance, to assess non-functional requirements such as "monitor and limit database growth" (NFR5) and "follow security procedures" (NFR2), we would need a close relationship with platform companies (e.g. via interviews or even by sending a request for information via institutions focused on children's online protection such as FairPlay for Kids, 5Rights Foundation or Alana Institute), as information available on the web (e.g. terms of use) or general use of the correspondent apps would not be sufficient to properly verify the companies conformance with such requirements.

The final step of our data collection, during the search process, involved the review of results by a single expert. This fact represents a possible threat to *external validity*, though we relied on his experience with the methodology (the second author had performed around ten mapping studies) and topic (in recent years, he supervised several students on children's rights, protection and security by tech companies).

6.3 Future Work

Our upcoming studies aim to enrich the set of requirements by analyzing gray literature (e.g. governmental reports, relevant IT news portals and large-circulation outlets, specialists' recommendations for Parental Control solutions providers, recognized non-governmental institutions, etc.) that could bring more features. We will also discuss the results with representatives of the two companies (i.e. Meta's Instagram and Bytedance's TikTok) based on collaboration with institutions such as the Alana Institute and Fairplay, which hold a direct

dialogue with such players. This will allow new rounds of application to provide us with better insight into how and if they need to be refined (e.g. combined, extended, split, better described, etc.)

Authors' Contributions

Author 1 contributions: conceptualization, data curation, formal investigation methodology, project administration, writing – original draft.

Author 2 contributions: conceptualization, data curation, formal investigation, methodology, project administration, validation, writing – original draft.

References

- Albuquerque, N., Valença, G., and Falcão, T. (2023). How social media platforms manipulate kidinfluencers? analysing the adoption of deceptive design patterns by big techs. In *Anais do XXII Simpósio Brasileiro sobre Fatores Humanos em Sistemas Computacionais*, Porto Alegre, RS, Brasil. SBC. DOI: <https://doi.org/10.1145/3638067.3638123>.
- Alrumaih, H., Mirza, A., and Alsalamah, H. (2020). Domain ontology for requirements classification in requirements engineering context. *IEEE Access*, 8:89899–89908. DOI: <https://doi.org/10.1109/ACCESS.2020.2993838>.
- Altarturi, H. H., Saadon, M., and Anuar, N. B. (2020). Cyber parental control: A bibliometric study. *Children and Youth Services Review*, 116:105134. DOI: <https://doi.org/10.1016/j.chilyouth.2020.105134>.
- BRAZIL (1988). Constituição da república federativa do brasil. <http://tinyurl.com/2ktersxk>, Accessed: 03 August 2024.
- BRAZIL (1990a). Lei nº 8.069. dispõe sobre o estatuto da criança e do adolescente e dá outras providências. <http://tinyurl.com/3jws2dej>, Accessed: 03 August 2024.
- BRAZIL (1990b). Lei nº 8.078. dispõe sobre a proteção do consumidor e dá outras providências. <http://tinyurl.com/46zs5r8z>, Accessed: 03 August 2024.
- BRAZIL (2014). Lei nº 12.965. estabelece princípios, garantias, direitos e deveres para o uso da internet no brasil. <http://tinyurl.com/ybep8f6d>, Accessed: 03 August 2024.
- BRAZIL (2018). Lei nº 13.709, lei geral de proteção de dados pessoais (lgpd). <http://tinyurl.com/64kc5j57>, Accessed: 03 August 2024.
- CGI.br (2023). Pesquisa sobre o uso da internet por crianças e adolescentes no brasil: Tic kids online brasil. <http://tinyurl.com/3y9y8py9>, Accessed: 03 August 2024.
- de Paula Albuquerque, O., Fantinato, M., Hung, P. C., Peres, S. M., Iqbal, F., Rehman, U., and Shah, M. U. (2022). Recommendations for a smart toy parental control tool. *The Journal of Supercomputing*, 78(8):11156–11194. DOI: <https://doi.org/10.1007/s11227-022-04319-4>.
- Fantinato, M., Hung, P. C. K., Jiang, Y., Roa, J., Villarreal, P., Melaisi, M., and Amancio, F. (2017). *A Survey on Purchase Intention of Hello Barbie in Brazil and Argentina*, pages 21–34. Springer International Publishing, Cham. DOI: https://doi.org/10.1007/978-3-319-62072-5_3.
- Ghosh, A. K., Hughes, C. E., and Wisniewski, P. J. (2020). Circle of trust: a new approach to mobile online safety for families. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–14.
- Mariya Stoilova, M. B. and Livingstone, S. (2024). Do parental control tools fulfil family expectations for child protection? a rapid evidence review of the contexts and outcomes of use. *Journal of Children and Media*, 18(1):29–49. DOI: <https://doi.org/10.1080/17482798.2023.2265512>.
- Matos, M. C. (2021). Redes sociais para crianças menores de 13 anos: qual o impacto? <http://tinyurl.com/sxpntwvy>, Accessed: 03 August 2024.
- Meta. Family center tools for instagram. <http://tinyurl.com/479uk88w>, Accessed: 03 August 2024.
- Meta. How services and tools from meta support age-appropriate experiences. <https://tinyurl.com/52hbetww>, Accessed: 03 August 2024.
- Meta. Instagram help center privacy settings & information. <http://tinyurl.com/479uk88w>, Accessed: 03 August 2024.
- Meta. Instagram help center: Tips for parents. <http://tinyurl.com/479uk88w>, Accessed: 03 August 2024.
- Meta. Instagram shopping feature. <http://tinyurl.com/ys4nc86b>, Accessed: 03 August 2024.
- Meta. Our tools, features and resources to help support teens and parents. <http://tinyurl.com/328afbay>, Accessed: 03 August 2024.
- Nouwen, M., Jafarinaimi, N., and Zaman, B. (2017). Parental controls: reimagining technologies for parent-child interaction. In *Proceedings of 15th European Conference on Computer-Supported Cooperative Work - Exploratory Papers*, pages 18–34. European Society for Socially Embedded Technologies (EUSSET). DOI: <https://doi.org/10.18420/ecscw2017-28>.
- Pasquale, L., Zippo, P., Curley, C., O'Neill, B., and Mongiello, M. (2022). Digital age of consent and age verification: Can they protect children? *IEEE Software*, 39(3):50–57. DOI: <https://doi.org/10.1109/MS.2020.3044872>.
- Penina, M. (2017). Telas e crianças: conheça os mitos e riscos desta exposição. <http://tinyurl.com/58waxr6y>, Accessed: 03 August 2024.
- Serra, A. C., Mendes, P. R. C., de Freitas, P. V. A., Bussion, A. J. G., Alan L. V. Guedes, and Colcher, S. (2021). Should i see or should i go: Automatic detection of sensitive media in messaging apps. In *Anais do XXVII Simpósio Brasileiro de Sistemas Multimídia e Web*, pages 229–236, Porto Alegre, RS, Brasil. SBC. <https://sol.sbc.org.br/index.php/webmedia/article/view/17495>, Accessed: 03 August 2024.
- Smirnova, S., Livingstone, S., and Stoilova, M. (2021). Understanding of user needs and problems: A rapid evidence review of age assurance and parental controls.
- TikTok. Tiktok: Guardian's guide. <http://tinyurl.com/yc49jkus>, Accessed: 03 August 2024.
- TikTok. Tiktok: Privacy and security on tiktok. <http://>

- tinyurl.com/yc7wjaum, Accessed: 03 August 2024.
- TikTok. Tiktok: Privacy policy for younger users. <http://tinyurl.com/mryrhxxz>, Accessed: 03 August 2024.
- TikTok. Tiktok: Safety privacy & controls. <http://tinyurl.com/yta2ukje>, Accessed: 03 August 2024.
- TikTok. Tiktok shop. <http://tinyurl.com/2p97prmd>, Accessed: 03 August 2024.
- TikTok (2019). Tiktok for younger users. <http://tinyurl.com/4vvpawnw>, Accessed: 03 August 2024.
- TikTok (2020). Tiktok introduces family pairing. <http://tinyurl.com/4j6cf4jc>, Accessed: 03 August 2024.
- Tove Lafton, J. E. B. W. and Holmarsdottir, H. B. (2024). Parental mediation and children's digital well-being in family life in norway. *Journal of Children and Media*, 0(0):1–18. DOI: <https://doi.org/10.1080/17482798.2023.2299956>.
- UNICEF (2019). Growing up in a connected world, unicef office of research – innocent, florence. <http://tinyurl.com/49rjnser>, Accessed: 03 August 2024.
- United Nations (1989). Convention on the rights of the child. <http://tinyurl.com/bddj4exw>, Accessed: 03 August 2024.
- Wisniewski, P., Ghosh, A. K., Xu, H., Rosson, M. B., and Carroll, J. M. (2017). Parental control vs. teen self-regulation: Is there a middle ground for mobile online safety? In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, CSCW '17, page 51–69, New York, NY, USA. Association for Computing Machinery. DOI: <https://doi.org/10.1145/2998181.2998352>.
- Zaman, B., Nouwen, M., Vanattenhoven, J., de Ferrer, E., and Looy, J. V. (2016). A qualitative inquiry into the contextualized parental mediation practices of young children's digital media use at home. *Journal of Broadcasting & Electronic Media*, 60(1):1–22. DOI: <https://doi.org/10.1080/08838151.2015.1127240>.

A Mapped studies

ID	Study
S1	V. Gnanasekaran, K. De Moor, Usability, security, and privacy recommendations for mobile parental control, in: Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference, EICC '23, Association for Computing Machinery, New York, NY, USA, 2023, p. 138–143. doi: https://doi.org/10.1145/3590777.3590800 .
S2	H. H. Altarturi, M. Saadoon, N. B. Anuar, Cyber parental control: A bibliometric study, <i>Children and Youth Services Review</i> 116 (2020) 105134. doi: https://doi.org/10.1016/j.childyouth.2020.105134 .
S3	W. Fuertes, K. Quimbiulco, F. Galarraga, J. L. Garcia-Dorado, On the development of advanced parental control tools, in: 2015 1st International Conference on Software Security and Assurance (ICSSA), 2015, pp. 1–6. doi: https://doi.org/10.1109/ICSSA.2015.011 .
S4	A. K. Ghosh, K. Badillo-Urquiola, M. B. Rosson, H. Xu, J. M. Carroll, P. J. Wisniewski, 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, CHI '18, Association for Computing Machinery, New York, NY, USA, 2018, p. 1–14. doi: https://doi.org/10.1145/3173574.3173768 .
S5	E. Magkos, E. Kleisiari, P. Chanias, V. Giannakouris-Salalidis, Parental control and children's internet safety: the good, the bad and the ugly, <i>Proc. ICIL 2014</i> 18 (2014).
S6	M. Nouwen, M. Van Mechelen, B. Zaman, A value sensitive design approach to parental software for young children, in: Proceedings of the 14th International Conference on Interaction Design and Children, IDC '15, Association for Computing Machinery, New York, NY, USA, 2015, p. 363–366. doi: https://doi.org/10.1145/2771839.2771917 .
S7	L. Rafferty, M. Fantinato, P. C. K. Hung, Privacy Requirements in Toy Computing, Springer International Publishing, Cham, 2015, pp. 141–173. doi: https://doi.org/10.1007/978-3-319-21323-1_8 .
S8	G. Wang, J. Zhao, M. Van Kleek, N. Shadbolt, Protection or punishment? relating the design space of parental control apps and perceptions about them to support parenting for online safety, <i>Proc. ACM Hum. Comput. Interact.</i> 5 (2021). doi: https://doi.org/10.1145/3476084 .
S9	A. Feal, P. Calciati, N. Vallina-Rodriguez, C. Troncoso, A. Gorla, et al., Angel or devil? a privacy study of mobile parental control apps, Proceedings of Privacy Enhancing Technologies (PoPETS) 2020 (2020). doi: https://doi.org/10.2478/popets-2020-0029 .
S10	M. Ko, S. Choi, S. Yang, J. Lee, U. Lee, Familync: facilitating participatory parental mediation of adolescents' smartphone use, in: Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous computing, UbiComp '15, Association for Computing Machinery, New York, NY, USA, 2015, p. 867–878. doi: https://doi.org/10.1145/2750858.2804283 .
S11	N. Sangal, D. Singhvi, M. Pharande, D. Patole, Teen-alyze: A mobile application for parental control, teen self-monitoring and active mediation, in: 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2021, pp. 1–5. doi: https://doi.org/10.1109/ICRITO51393.2021.9596148 .
S12	P. Wisniewski, A. K. Ghosh, H. Xu, M. B. Rosson, J. M. Carroll, Parental control vs. teen self-regulation: Is there a middle ground for mobile online safety?, in: Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, CSCW '17, Association for Computing Machinery, New York, NY, USA, 2017, p. 51–69. doi: https://doi.org/10.1145/2998181.2998352 .
S13	M. Nouwen, N. Jafarainaimi, B. Zaman, Parental controls: reimagining technologies for parent-child interaction, in: Proceedings of 21 15th European Conference on Computer-Supported Cooperative Work- Exploratory Papers, European Society for Socially Embedded Technologies (EUSSET), 2017, pp. 18–34. doi: https://doi.org/10.18420/ecscw2017-28 .
S14	S. Wardhana, M. K. Sabariah, V. Effendy, D. S. Kusumo, 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 (ICoICT), 2017, pp. 1–6. doi: https://doi.org/10.1109/ICoICT.2017.8074715 .
S15	O. d. P. Albuquerque, M. Fantinato, S. M. Peres, F. Iqbal, P. C. Hung, A conceptual model for a parental control tool for smart toys, in: 23rd International Conference on Artificial Intelligence, 2021, pp. 1–10.
S16	L. Gonçalves de Carvalho., M. Medeiros Eler., Security requirements for smart toys, in: Proceedings of the 19th International Conference on Enterprise Information Systems - Volume 2: ICEIS, INSTICC, SciTePress, 2017, pp. 144–154. doi: https://doi.org/10.5220/0006337001440154 .
S17	O. de Paula Albuquerque, M. Fantinato, P. C. Hung, S. M. Peres, F. Iqbal, U. Rehman, M. U. Shah, Recommendations for a smart toy parental control tool, <i>The Journal of Supercomputing</i> 78 (2022) 11156–11194. doi: https://doi.org/10.1007/s11227-022-04319-4 .
S18	H. Ameer, A. Rekik, S. Jamoussi, A. B. Hamadou, Childprotect: A parental control application for tracking hostile surfing content, <i>Entertainment Computing</i> 44 (2023) 100517. doi: https://doi.org/10.1016/j.entcom.2022.100517 .

ID	Study
S19	Z. İftikhar, Q. R. u. Haq, O. Younus, T. Sardar, H. Arif, M. Javed, S. Shahid, Designing parental monitoring and control technology: A systematic review, in: C. Ardito, R. Lanzilotti, A. Malizia, H. Petrie, A. Piccinno, G. Desolda, K. Inkpen (Eds.), <i>Human-Computer Interaction – INTERACT 2021</i> , Springer International Publishing, Cham, 2021, pp. 676–700.
S20	K. Badillo-Urquiola, D. Smriti, B. McNally, E. Golub, E. Bonsignore, P. J. Wisniewski, Stranger danger! social media app features co-designed with children to keep them safe online, in: <i>Proceedings of the 18th ACM International Conference on Interaction Design and Children, IDC '19</i> , Association for Computing Machinery, New York, NY, USA, 2019, p. 394–406. doi: https://doi.org/10.1145/3311927.3323133 .
S21	Y. Hashish, A. Bunt, J. E. Young, Involving children in content control: a collaborative and education-oriented content filtering approach, in: <i>Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '14</i> , Association for Computing Machinery, New York, NY, USA, 2014, p. 1797–1806. doi: https://doi.org/10.1145/2556288.2557128 .
S22	S. Yardi, A. Bruckman, Social and technical challenges in parenting teens' social media use, in: <i>Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '11</i> , Association for Computing Machinery, New York, NY, USA, 2011, p. 3237–3246. doi: https://doi.org/10.1145/1978942.1979422 .
S23	L. Zhang-Kennedy, C. Mekhail, Y. Abdelaziz, S. Chiasson, From nosy little brothers to stranger-danger: Children and parents' perception of mobile threats, in: <i>Proceedings of the The 15th International Conference on Interaction Design and Children, IDC '16</i> , Association for Computing Machinery, New York, NY, USA, 2016, p. 388–399. doi: https://doi.org/10.1145/2930674.2930716 .
S24	D. Sarwatay, J. Lee, D. B. V. Kaye, Exploring children's tiktok cultures in india: Negotiating access, uses, and experiences under restrictive parental mediation, <i>Media International Australia</i> 186 (2023) 48–65. doi: https://doi.org/10.1177/1329878X221127037 .
S25	A. MAFTEI, I.-A. MERLICI, How should children and adolescents use digital devices in a healthy manner, and how should parents employ digital control?, <i>International Journal of Social and Educational Innovation (IJSEIro)</i> 10 (2023) 134–165.
S26	M. Kumar, V. Dwivedi, A. Sanyal, P. Bhatt, R. Koshariya, Parental security control: A tool for monitoring and securing children's online activities., in: <i>Proceedings of the 2021 Thirteenth International Conference on Contemporary Computing, IC3-2021</i> , Association for Computing Machinery, New York, NY, USA, 2021, p. 469–474. doi: https://doi.org/10.1145/3474124.3474196 .
S27	Marsh, An Examination of Parenting Strategies for Children's Online Safety), Ph.D. thesis, Carnegie Mellon University, Pittsburgh, PA, USA, 2018. doi: https://doi.org/10.1184/R1/7188881.v1 .
S28	M. Stoev, D. K. Sarmah, Online protection for children using a developed parental monitoring tool, in: X.-S. Yang, R. S. Sherratt, N. Dey, A. Joshi (Eds.), <i>Proceedings of Eighth international Congress on Information and Communication Technology</i> , Springer Nature Singapore, Singapore, 2023, pp. 205–215. doi: https://doi.org/10.1007/978-981-99-3243-6_17 .
S29	P. Dias, R. Brito, Criteria for selecting apps: Debating the perceptions of young children, parents and industry stakeholders, <i>Computers & Education</i> 165 (2021) 104134. doi: https://doi.org/10.1016/j.compedu.2021.104134 .
S30	S. Çankaya, H. F. Odabasi, Parental controls on children's computer and internet use, <i>Procedia - Social and Behavioral Sciences</i> 1 (2009) 1105–1109, world Conference on Educational Sciences: New Trends and Issues in Educational Sciences. doi: https://doi.org/10.1016/j.sbspro.2009.01.199 .
S31	B. McNally, P. Kumar, C. Hordatt, M. L. Mauriello, S. Naik, L. Norooz, A. Shorter, E. Golub, A. Druin, Co-designing mobile online safety applications with children, in: <i>Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, CHI '18</i> , Association for Computing Machinery, New York, NY, USA, 2018, p. 1–9. doi: https://doi.org/10.1145/3173574.3174097 .
S32	T. Warner, C. Meadows, P. Wahjudi, Analysis, recognition, monitoring, and reporting tool (armr), <i>Journal of Management & Engineering Integration</i> (2012).
S33	M. B. Mariya Stoilova, S. Livingstone, Do parental control tools fulfil family expectations for child protection? a rapid evidence review of the contexts and outcomes of use, <i>Journal of Children and Media</i> 18 (2024) 29–49. doi: https://doi.org/10.1080/17482798.2023.2265512 .

B Requirements per Studies

Table 2. Analysis of evidence for each functional requirement on TikTok.

Requirement	Studies' IDs
FR1 - allow children and parents to report inappropriate content	S20 S29 S31
FR2 - allow children to ask for help	S12 S20
FR3 - automatically detect and warn about risky content	S20 S31
FR4 - provide features to help using the tool	S1 S13 S14 S15 S17
FR5 - raise children and parents' awareness about online security	S1 S7 S8 S9 S12 S15 S17 S19 S23
FR6 - provide communication channels to promote the discussion among parents, children and the platform	S1 S19
FR7 - provide features and guidance materials to raise parents-children dialogue	S20
FR8 - allow parents to monitor children's activities	S1 S2 S4 S5 S8 S11 S12 S15 S17 S18 S19 S20 S22 S23 S28 S30 S31 S32 S33
FR9 - enable children's self-monitoring and regulation	S8 S11 S19 S20 S27
FR10 - allow parents to block or filter activities and/or content accessed by the child on the platform	S2 S3 S5 S8 S12 S18 S19 S20 S21 S22 S24 S25 S26 S27 S28 S29 S30 S31 S33
FR11 - allow parents to link their profiles to the child's account through authentication mechanisms	S1 S16 S17 S20 S23 S33
FR12 - allow parents to authorize financial transactions	S17
FR13 - obtain parental consent for using child's data	S15 S16 S17 S29 S33
FR14 - allow parents to access and manage (delete or restrict) their children's data on the platform	S1 S7 S9 S15 S16 S17
FR15 - allow parents and children to create and manage privacy rules	S15 S17 S23
FR16 - notify security breaches	S17
NFR1 - monitor the children's activity in a non-intrusive way	S1 S7 S8 S19 S20 S27
NFR2 - follow regulations and security standards and procedures	S1 S7 S9 S17
NFR3 - platforms should not allow third-party services to collect children's data	S9
NFR4 - consider data minimization and outgoing content blocking	S7 S16 S30
NFR5 - monitor and limit database growth	S16
NFR6 - require digital certificate for mobile services	S16 S17
NFR7 - maintain application settings every time parents or children use it	S16 S17
NFR8 - encrypt personal information	S16 S17
NFR9 - restrict access to essential files on the phone	S16
NFR10 - ensure accuracy of personal information	S16
NFR11 - provide support to multiple platforms	S1 S3 S17
NFR12 - provide parents with flexible and varied functionalities for parental control	S1 S4 S7 S19 S20 S23 S27
NFR13 - address parents' needs	S7 S17 S19 S27