Privacy-Enhanced Parenting Mediation System "ProKids" Providing Age-Appropriate Content with X.509 Certificate Age Rating

Juehee Dawson

Thesis submitted to the University of Ottawa
in partial Fulfillment of the requirements for the
Master of Applied Science Degree
in Electrical and Computer Engineering

School of Electrical Engineering and Computer Science
Faculty of Engineering
University of Ottawa

Abstract

It is desirable that children access the Internet for playing and learning, however, increasing inappropriate content poses various threats to children. Such threats do not just include security and privacy risks but also risks of long-term mental and physical harm. Technical mediation tools available to support parents in controlling and monitoring their children's online activity may not sufficiently balance recommended parenting mediation strategies. Recent legislative changes related to children's online security and privacy have caused the industry to implement new solutions, but these are weak in data privacy.

We propose a parenting mediation tool, designed with privacy, age ratings, and Teen Online Safety Strategies (TOSS) using the Value Sensitive Design (VSD) approach. The design includes stakeholders in children's digital ecosystem as main actors (i.e., government/governance authorities, content providers, parents/guardians and children), and it utilizes the X.509 certificate extension field to represent the age-rating of the content. The tool authorizes the websites by verifying the X.509 certificates to provide age-appropriate content to children. *ProKids* offers data privacy and age-appropriate content by design while offering differentiated design for younger and older children to support children's growing autonomy. *ProKids* was evaluated by an initial exploratory user study and a comparison analysis against existing studies and industry-provided tools. This thesis revealed that the existing tools function well in control and monitoring but are weak in privacy, do not provide consistent age-appropriate content and most do not support teen self-regulation strategies. This thesis found that more support for children in the transitional age group (of 10-12) may be beneficial. The most important values parents indicated they cared about in parental mediation tools were 1) content, 2) interaction with others, 3) privacy, 4) transition age, 5) consistent ratings, 6) education and communication, and 7) trust. Patterns of how parents mediate their children online were 1) restrictive and monitoring (when kids are young), 2) active mediation (use of communication and education), 3) neglectful with a feeling of helplessness in terms of external support and no control when kids get older. Parents liked the content rating and privacy features of *ProKids* and the system was very well received by parents.

Acknowledgements

I express my gratitude and thoughts to those who supported and inspired me throughout my study.

My two lovely children were huge sources of inspiration for this thesis. Thank you for being good, genuine, curious and playful. I look forward to spending more evenings and weekends with you.

I am thinking of my dear brother, Ju Sung and my grandfather both of whom passed away during my study. They had so much love and grace, demonstrating the essence of lives well lived and they will keep me inspired for years to come.

The study was not easy to pursue with so many unexpected obstacles in life as well as the COVID-19 pandemic. I am so grateful for my close friends who kept motivating me with kind words and prayers, and my work supervisors who supported me by being so flexible with ever-changing work schedule arrangements.

I am grateful for my loving husband who supported me by believing in me and helping take care of our children throughout the study.

Lastly, I am very thankful for my thesis supervisor Professor Adams, for his wisdom, patience and assistance in guiding me through the program and keeping me on track.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

The Internet was created to connect people and has become essential for so many different purposes in our everyday lives that it is almost unthinkable to consider living without it today. New Internet technologies and emerging services have opened up a new world for everyone by providing convenience, entertainment and endless resources, but they have also created new kinds of threats and risks to all users – including our children.

Over 175,000 children are going online for the first time every day globally to learn, have fun and grow, the number of hours spent online is growing rapidly, and the age at which children access mobile devices is getting younger [1][2]. There have been global surges in online content and applications being accessed by children including language apps, virtual tutoring, video conferencing tools, and online learning software since the global emergence of COVID-19 and these phenomena of children using more technologies online every day are here to stay [1][3].

This chapter introduces the motivation and the goal of the study starting by glancing at how these digital environments are affecting children and how children are being supported in the environments.

1.1 Online Opportunities and Threats to Children

"Safety and security don't just happen, they are the result of collective consensus and public investment. We owe our children, the most vulnerable citizens in our society, a life free of violence and fear." – Nelson Mandela

---

Children use the Internet by watching videos, playing games, doing homework or socializing with their peers. They are increasingly surfing the web with their mobile devices, always being online and reachable. Most parents have positive views on their children's screen media use as tools for learning, and socializing when they spend the 'right amount of time'. Parents worry about the content their children access being violent, sexual, or involving drug use or cyberbullying. They also worry about ads, the collection of private information as well as interactions with strangers via games, social network sites (SNS), and video-sharing sites as these service platforms and systems keep evolving [2],[4]. Other concerns involve the unregulated use of the Internet which can disrupt children's sleeping, physical activity, study and family time [5].

Fernandes et al. [3] introduced a taxonomy that identifies 45 possible online threats to children and adolescents as shown in Figure 1.1. The threats categories include advantages, confusion, content against human rights, cyberbullying, funny and disturbing, inappropriate content, navigating risks, online extortion, online predators, privacy breaches and threats about identity, sexuality and self-affirmation. Note that *inappropriate content* and *navigation risks* categories are associated as they can link to one another.

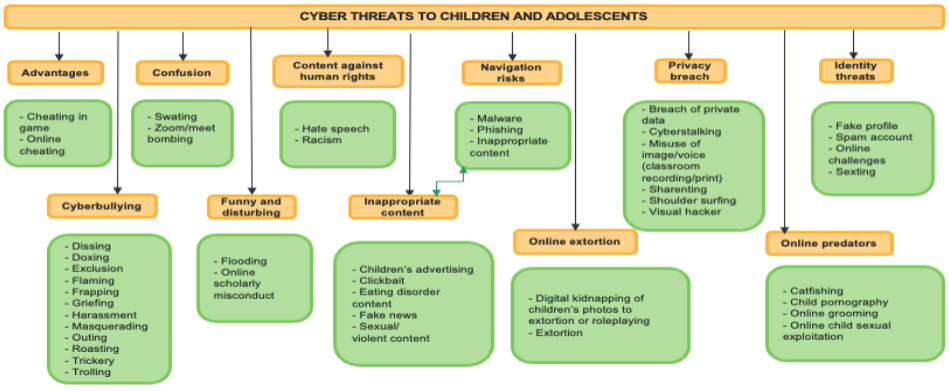


Figure 1.1 Taxonomy of cyber threats involving children and adolescents [1]

[1] See Glossary for term descriptions.

Hartikainen et al. [6] categorized the Internet threats for children in four categories.

1) *Content threats*:

They include inappropriate content such as commercial spam, targeted emails/ads, adult abusive content such as pornography, violence, pro-anorexia and drug related content.

2) Contact threats:

Contact threats include grooming, sexting, cyberbullying, cyberstalking and privacy loss.

3) Conduct threats:

Situations where children engage in disapproved or illegal activities such as illegal file sharing or bullying others.

4) Computer/Internet threats:

They include information security threats like malware, data theft/loss, password stealing/cracking but also Internet addiction.

Some of the consequences of exposure to these threats are as follows:

1) Accessing inappropriate content:

Inappropriate content may contain harmful information such as portrayals of graphic violence, pornography, self-harm or hate speech, but it can also be related to inappropriate design and improper age verification. For example, youth purchased more cigarettes online without proper age verification since 2019 [7]. Online shopping sites enable kids to purchase items they are not allowed to purchase in person (see Figure 1.2). Kids are also exposed to

content with ads and popups that include dark patterns[2]. The concerns around dark patterns are still developing [8], [9]. That said, it has been seen that children having unintentionally accessed inappropriate content, sometimes via dark patterns, often wished they could have been blocked. Yet, once they had accessed inappropriate content, they often returned to these sites with an increasing frequency [10].

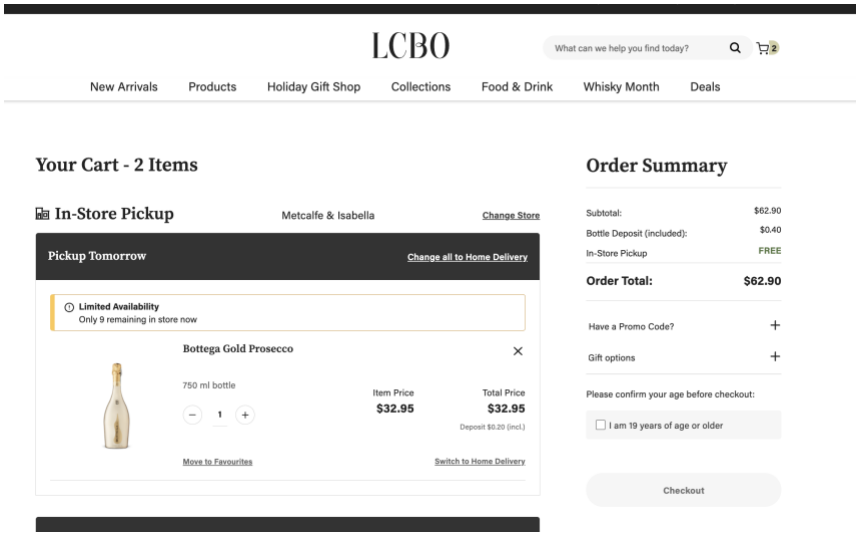


Figure 1.2 Example of weak age verification in age-inappropriate content

2) Mental health effects:

Viewing content designed for older audiences can increase fear and anxiety in younger children, and excessive media exposure in children can increase attention disorder [11]. Social media is said to contribute to mental health crises among young people [12].

[2] See Glossary for the description of dark patterns.

3) Sexual abuse:

Some 80% of children reported feeling in danger of sexual abuse or exploitation while online and one in three children was exposed to sexual content online [13].

4) *Security/privacy concerns*:

Stories of companies mishandling or sharing children's private information with third parties are not new [14], [15], [16]. Personal data shared with websites or service platforms can be transferred to third parties without the user realizing the transfer has happened. Many game websites that children access store sensitive information such as device credentials, payment information, phone numbers and email addresses [17]. This type of implicit data transfer raises greater privacy concerns than those initiated by the user [18]. Dark patterns are often discussed in terms of ethics or values, but they are security and privacy concerns as well. Dark patterns that lure adults, target the vulnerable sub-populations like children. The early childhood market is a Wild West, with many apps appearing more focused on making money and invasive data collection than on children's play experience [9], [19], [20], [21]. The emergence of unregulated technologies such as smart devices in the Internet of Things (IoT) and Artificial Intelligence (AI) only increase concerns with respect to children's security and privacy in the digital world and the urgency of pursuing policies and guidelines for age-appropriate design [5], [22].

1.2 Supporting Children

"It takes a village to raise a child." – proverb

Protecting children to be safe while they benefit from the Internet requires an effort from all stakeholders including parents, schools, industry and governments as well as children themselves. Acknowledging that digital safety requires a range of deliberations balancing legal, policy, ethical, social and technological considerations is vital. Multi-stakeholder cooperation is required to create a safer digital ecosystem for children [18], [23], [24], [25].

Many parents and schools rely on parental control solutions that are easily accessible either for free, or for a relatively inexpensive price. They can be categorized as standalone devices (e.g., Asus router), operating system and device-specific (e.g., Apple, Google or Android), or age-related content platforms (e.g., YouTube Kids, Netflix Kids, or Roblox). Although the number is low (i.e., less than 30%), a growing portion of parents use these parental control solutions and they prefer solutions that come with easy setup, good default settings and a lower cost [2], [26]. Each tool is different and works well for a specific purpose if properly chosen and configured well, but there is no single perfect tool that works well for every function [17], [27]. There are often security and privacy concerns around the parental control tools for children and parents due to improper access control and insecure data transfer or storage [27], [28], [29]. The industry-provided parental tools specifically designed to protect children, often target children as an untapped market and collect private data such as identity and/or online behaviour [2], [30], [31].

There are efforts by the industry to provide solutions for children. Parental control tools and age-limited content have been introduced by service platforms (e.g., *Google Family Link*, *Apple Parental Control*, *Microsoft Family Safety*, etc.) and applications (e.g., *YouTube Kids*, *Netflix Kids*) that children access. Companies like Google, Snapchat, and Twitter work closely with law enforcement, governments and Non-Governmental Organizations (NGO) to develop tools for the safety of children online [23]. These tend to work well for certain functionalities such as restricting content, but the age limitation methods are found to have weak defaults and too many

loopholes that children can use to get around them [6]. Figure 1.3 shows an example of Google parental control settings page including private information.

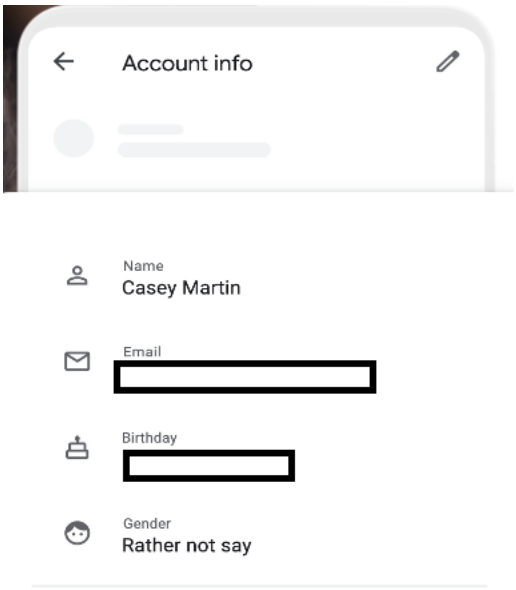


Figure 1.3 Example of Google's parental mediation tool collecting children's data

There are also efforts from supportive governments around the world, which we discuss in detail in section 2.1.2.3. They introduce industry requirements to implement proper age-verification methods on websites.

Currently, the age-verification methods implemented on some adult-oriented sites are too weak or pose further privacy concerns [31]. Measures such as age estimation tools or scanning devices for age-appropriate experience can impact user privacy.

1.3 Motivation

"It is easier to build strong children than to repair broken men" – Frederick Douglass, abolitionist and statesman

This thesis proposes a system called *ProKids* to enhance children's safe online experience using a more private parental mediation tool that enables age-appropriate content by default design. Parental interventions that mainly focus on mitigating online risks overlook the possibilities of exploring and learning about and through media by children, which has been termed as *online opportunities* by Livingstone et al. [32], [33]. Parental mediation refers to the strategies that parents take during their children's media use to minimize the risks and maximize the benefits of media on their children [34]. To overcome the negativity associated with vocabulary *control* or *monitoring* [35] and also with the aim of combining all recommended parenting mediation strategies in the tool, we call our system a parental *mediation* tool. Various categories of parenting mediation strategies and recommendations are found in Chapter 2.

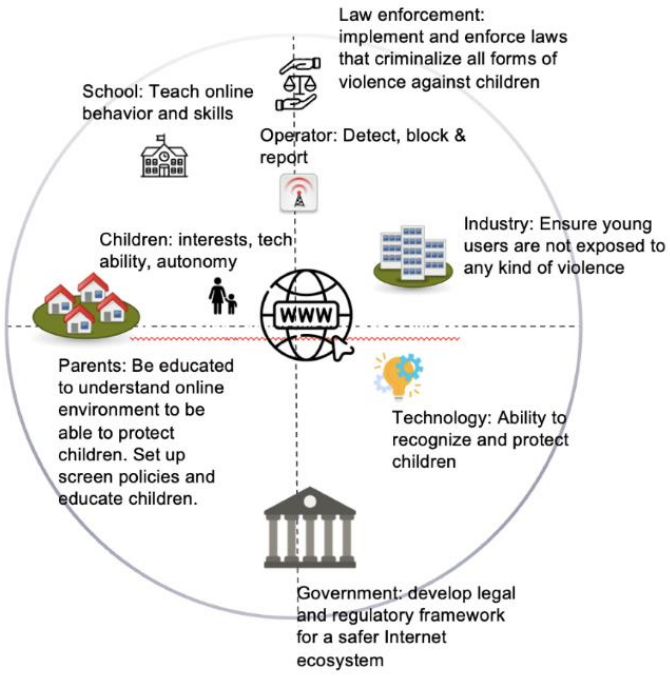


Figure 1.4 Safer Internet ecosystem

The Internet is like a jungle. We send kids into the wild blindly hoping they are not caught by wild animals. Can we instead design a system like a safety zone (for example, like a school) where we can send them knowing they are in a safe boundary instead of constantly keeping up with confined allow/block lists of URLs? *ProKids* helps parents mediate children more effectively with less maintenance and helps children explore the safer Internet with a focus on building their autonomy. The system design involves all the key stakeholders including parents, the industry and regulators (or governance) [23] (See Figure 1.4). We use X.509 certificates as a technology medium between home and industry and try to reduce the gaps between new government policies and their implementation while providing more data privacy to families. The mediation tool, implemented in a desktop browser, enables parents to mediate their children using a recommended balanced combination of three mediation strategies and with differentiated features for teens to promote autonomy.

Value Sensitive Design (VSD) [35], [36] is a theoretical technology design approach that accounts for human values in a principled and comprehensive manner throughout the iterative design process. The details of VSD are found in section 2.2. We built the system based upon the VSD approach [36], [37], an empirical investigation was carried out as an initial exploratory user study with 12 parents of 22 children under age 18. The proposed system received feedback from parents, and was compared to other parental mediation tools. *ProKids* was accepted positively by all parents in the study who tended to indicate that the Internet needed increased governance to protect children.

1.4 Study Goals and Contribution

The aim of the thesis was to design a proof of concept system that enabled the provision of age-appropriate content for children with enhanced data privacy.

The following goals were achieved by the system:

- *Privacy*

  The user setting data stays in the device so that the user information and their monitoring data are not shared externally.

- *Age ratings as prevention*

  The system provides age rating features that allow consistent content ratings and viewing experience. A user does not have to rely on a content provider to verify (fetch data) his/her age but instead, the user's browser employs ProKids to verify the age rating of the site.

- *Safer environments*

  The additional parenting mediation features help parents mediate children in a more balanced way while not having to maintain lists of where they can and cannot go.

- *Explore and learn*

  Children can explore the Internet themselves and learn and freely browse more websites instead of being too tightly restricted.

- *Acceptance*

  The initial exploratory user study that was conducted showed that parents liked *ProKids* for privacy and default age ratings features.

The study contributed to the following areas:

- The study made efforts to reduce gaps in the current digital ecosystem for children. It provided a proof of concept system showing how X.509 certificates can be used to provide age-rating verification mechanisms for web content. While this does not nullify the age-verifying requirements for adult sites, it can mitigate security and privacy harm to children by preventing them from accessing such sites.
- We designed the privacy model of *ProKids* by combining recommended approaches [18], [38], [39]. The comparison analysis of privacy risks and privacy design strategies revealed high privacy risks and improper privacy architecture in most existing tools. The risks and privacy design strategies to counter them are mentioned in sections 2.3.4 and 2.3.5 respectively.
- The proposed system design model expands the Teen Online Safety Strategies (TOSS) values to include privacy and age ratings. The description of the TOSS framework is found in sections 2.1.1.3.
- The initial exploratory user study with parents showed the distinct challenges they have with children in the transitional group (10-12 years old). While this could be a sensitive age group, there was no other study we are aware of mentioning this age group in particular.
- The initial exploratory user study results showed the patterns of parents' mediation styles as children grow. They were controlling and restricting manually over the shoulder when children were young, and they became neglectful while feeling passive and vulnerable (rather quickly) when children were tweens or teens. Supporting children to safely learn

and explore on the Internet while they are still young is the missing step. *ProKids* is designed to help with this part.

Chapter 2

Background

This chapter investigates different parenting mediation styles that are practiced and different technical approaches that have been developed to enhance children's online experience. We also discuss *VSD*, a theoretical design framework as well as the X.509 certificate as they are used in the proposed system. The related literature of parental mediation tool design then follows.

2.1 Concepts around Parental Mediation Tools

2.1.1 Parental Mediation Strategies

This section discusses various parental mediation strategies and context considerations from the existing works, and the strategies this thesis considered in the scope of the *ProKids* design.

2.1.1.1 Mediation Strategies Categories

Studies categorized different mediation styles. Much of the work regarding parental mediation strategies online safety was originally derived from Valkenburg et al.'s study [40] which assessed three styles of parental television mediation consisting of *social-co-viewing, restrictive* and *instructive* [34]. Collier et al. [41] categorized three different mediation styles as *restrictive, active* and *co-viewing* and their effects on the children in the long term. Livingstone et al. [32] studied the parental mediation styles of how they find the "holy grail" of optimizing the online opportunities for children while minimizing online risks and found two distinct mediation styles, *restricting* and *enabling*. Wisniewski et al. [42] identified the primary parental mediation strategies as *monitoring, restriction* and *active mediation* as part of Teen Online Safety Strategies (TOSS). Yu et al. [34] categorized parents' mediation practices in three dimensions including 1)

creative mediation, where parents mediate to support children's creating and learning with media, 2) *preparative mediation*, where parents explore and prepare media for children's engagement and 3) *administrative mediation*, where parents administer and regulate their children's media use to highlight various supportive practices in children's learning and creative activities.

2.1.1.2 Mediation Context

Many studies found that parents' decision making process in parental mediation is influenced by different factors such as age, gender and socio-economic status of parents, ethnography, age and gender of kids and consequences associated with each parental mediation style such as perception of children about digital media, development degree of digital skill and literacy [24], [43], [44]. For example, enabling mediation is done to more digitally skilled kids and parents who practice enabling mediation are more aware of online risks. Restrictive mediation is done to more girls, younger and less skilled children. Mothers restrict more than fathers, more digitally skilled parents and older parents use restrictive mediation. Parents with higher risk perception do more enabling and restrictive mediation and low-income families are more opportunity-focused rather than risk-focused [32], [44].

Our proposed system provides flexible decision-making options for parents considering different family contexts.

2.1.1.3 Recommended Approaches

Collier et al. [41] emphasized the importance of parents' need to educate themselves on the harmful and beneficial effects of media and appropriate parenting such as creating rules for media use and discussing character's choices. Studies have recommended combining the right amount of active mediation with restrictive mediation to build a safe framework so that children's positive uses of the Internet can be encouraged [32], [45].

A. *Teen Online Safety Strategies (TOSS)*

The TOSS [42] framework conceptualizes the dichotomy between parental control and teen self-regulation in the context of children's online safety around the primary parental mediation strategies and teens' self-regulation strategies with the goal of promoting the online safety of children as shown in Figure 2.1.

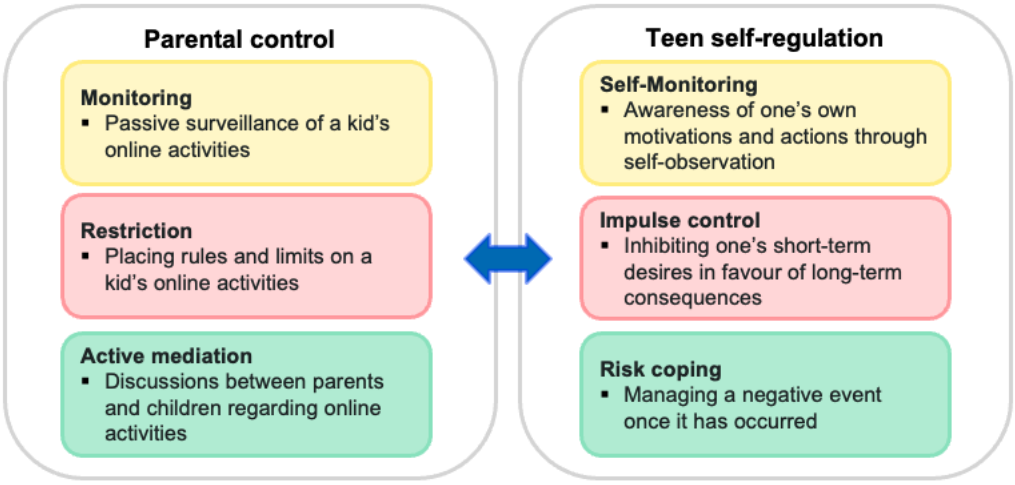


Figure 2.1 TOSS strategies for parental control and teen self-regulation

The framework has been used in many studies around children's online safety efforts. It was originally derived to illustrate the tensions between parental control and teen self-regulation when it comes to teens' online behaviours, their desires and online safety. The TOSS framework was developed by analyzing app features of 75 Android apps promoting teen mobile online safety.

This thesis employs the parental mediation strategies from TOSS because the TOSS categories make the functionality analysis of the mediation tools clearer and they have been used in many studies of parental mediation tools [26], [45]. **Error! Reference source not found.** shows how they are considered in our system's design.

2.1.2 Technical Mediation

This section discusses how technical mediations are designed to help children browse safer online but are not always useful in preventing children from accessing harmful content. Furthermore, we discuss that age-appropriate content design which differentiates age groups, is recommended, and we also discuss how new government policies require age-appropriate content design. Age-rating governance of other media types is shown at last.

2.1.2.1 Parental Mediation Tools

Parental control software enables parents to support risk management of their children's digital media use [46].

While there are many technical mediation tools available, they are not widely used [42], [47]. Parents find these technologies burdensome, ineffective, and often too rigid for their lives. They also struggle to enforce the rules with their children, especially teens. There can also be usability issues including technical difficulties, targeting different age audiences, and an inability to locate relevant apps [26], [42], [47], [48]. Parents want to balance restrictions and opportunities but most apps do not support active, engaged and supportive parenting [42]. The tools' blocking or filtering features are not very effective with an under-blocking rate (i.e. the rate at which material that should be blocked is missed) that is higher than 30% [27]. The report by the European Commission [27] also showed that most of the PC tools are easy to install and configure but difficult to customize to one's own needs. Too many options make the risk of unwanted configuration effects and bad filtering results high. The content filtering for different ages is not consistent with most tools (e.g., no difference between <12 and >13 although the categories exist or under/over blocking). They also mention that traditional block list filtering is not enough as the tools have difficulties with user-generated content and Web 2.0 content. All

tools allowed loophole access to harmful content (e.g., access to harmful content through Google Translate) [27].

Our study aims to design a system that can be widely used and works effectively to protect children including teens from harmful content without technical burden to the parents while supporting active, engaged and supportive parenting.

2.1.2.2 Age Groups

Studies suggest differentiated mediation approaches are required for children in different age groups [49]. For mediation tools, it is recommended to design features considering age groups and balancing the parental mediation strategies while supporting autonomy as children get older [42].

A. *Young children under 10 years old*

   For younger children, using restrictive measures is recommended as they have higher risks when exposed to inappropriate content. Viewing content designed for older audiences can increase fear and anxiety in younger children, and excessive media exposure in these young children can increase attention disorder [11]. Restrictive mediation is recommended for very young children.

Defining the age groups for parental mediation tools is not an easy task. Proper consideration of children's age and development stages is necessary [49].

According to [4], parental co-use goes down dramatically as the child's age goes up. More than two-thirds of 5-8 year old had their own mobile devices. 90% of this age group who watch online videos, the children themselves were most likely to select what to watch, either through their own searching, auto play or 'suggested' videos on the platform.

Piaget's theory of cognitive development theory [50] had three age groups - ages 2-6 (preoperational), 7-12 (concrete operational), and older than 13 (formal operational).

Yadav et al. [51] studied the patterns of inappropriate content accessed and the recommended mediation strategies by age groups as shown in Table 2.1.

Table 2.1 Mediation strategies for young children

Age group	**Contents**	**Risks**	**Development stage**	**Mediation strategy**
4-6 years	Voice search to find their favorite toys, games and cartoons.	• Search results in unsuitable contents. • Click unintentionally on advertisement, notifications from apps, opening adult and violent content.	• Learning skills. • Lack of awareness.	Use appropriate measure to advise them to refrain from clicking on random sites.
7-8 years	Search for games, actions and other videos of their choices.	• Exposure to adult and violent content via pop-up advertisements. • Long term impact on their behavior from exposure to gruesome violent videos.	• Awareness of certain videos. • Not mature enough to understand the risks.	Intervention to steer away from dangerous content.

9-10 years	Explore with random purposes and visit the unknown sites.	• Intentionally click on violent content links. • Prone to be subjected to online hazards as they explore on their own more.	• Confident on digital functionalities. • Prefer to watch content with graphics rather than texts.	Extreme caution for their psychological well-being. Advise with subtle warnings and suitable rewards for children.

B. Children over 10 years old

When it comes to teens, a more balanced approach is recommended. While young children accept certain restrictions upon education and proper interactions, teens' need for privacy is directly tied to their need for autonomy and respect [48]. Too much restriction often results in tension between parents and teens [4], [52]. And because of this very reason, some studies question the effectiveness of using parental mediation tools at all. Nouwen et al. [33] suggested acknowledging the different views and roles children and parents have in children's digital media use and the tool designers should allow prolonged negotiations, and think of ways to enrich data on children's online activities by providing families with clues on how to engage with each other.

Using parental control for only restriction with teens has adverse effects creating tension between parents and children. The design of apps and websites teens access should promote safety through engagement rather than restrictive parenting [53]. Wisniewski et al. [42] found that 89% of features in the 75 apps analyzed supported parental control while only 11% of the features supported teen self-regulation. Less than 1% supported

parental active mediation and teen impulse control. Tweens and teens begin to separate from their parents. They negotiate their relationships with their parents and assert their autonomy while they continue to rely on their parents for support and guidance. Badillo-Urquiola et al. [35] worked with adolescents to create an online safety app using VSD and the app emphasized safety, parent-teen communication, teen autonomy and privacy and parental support. Kawas et al. [54] provided design guidelines to create opportunities for technology to reduce family screen-time tension by guiding clear limit settings, eliciting a meaningful rationale for limits, mitigating conflicts by acknowledging tweens' perspectives and providing choices and options.

This section showed that more active mediation is recommended as tweens and teens still require guidance and protection while supporting their autonomy is necessary. Taking the recommendation of the studies above, our proposed system allows age-appropriate content by age ratings and the design differentiates between children under 10 and above.

2.1.2.3 Age-appropriate Design and Policies

Developing policies that both safeguard and empower children in the digital world is challenging [55]. A range of child protection measures have been designed to mitigate the content, contact and conduct risks children encounter online.

The comparisons and gaps between countries with different levels of public support in the European Union (EU) have been studied by O'Neil [56]. The recommended implications are:

1) The policy should support a broad spectrum of activities involving multiple stakeholders rather than a single solution.

2) Coordination, whether undertaken by a designated agency or multi-stakeholder representative body, is a key element in ensuring effective policy development.
3) Every country has a different starting point when it comes to policy implementation and sharing good practices and learning from what works best is crucial.

Current technology trends of children and policy developments in Organization for Economic Cooperation and Development (OECD) countries have been studied by Graafland et al. [55]. While these authors emphasized the importance of legal policies, they also mentioned alternatives to protect children online such as using technologies or self-and co-regulation measures that influence the behaviour of market actors. For example, Social Networking Services (SNSs) may contribute to children's online safety by improving default privacy settings, introducing accessible 'report abuse' buttons, or setting age limits for creating user accounts. They mention filtering technology, age or identification verification and walled gardens (i.e., child safety zones on the Internet) as technological measures.

This section discusses the recent development of strategies for children online in some countries.

A. European General Data Protection Regulation (GDPR) (2018)

The GDPR protects the rights and freedoms of all natural persons including children. The EU regulator considered it important to highlight that the protection of children deserves careful consideration related to controllers dealing with children's sensitive personal data. It tasked supervisory authorities with undertaking activities to create awareness and understanding of risks, safeguards and rights, with special attention to children [31].

B. Digital Services Act (DSA) (2022)

The DSA is an EU Act that concerns everyone where digital services must protect users' rights and not share private data. It has a special section for minors to make sure their services offer a high level of privacy, safety and security to young users. A risk assessment process assesses the online risks for digital services every year and requires the platforms to have parental control settings, age verifications and reporting tools. It also forbids content providers to use *dark patterns* in their services [57].

C. EU Code of Conduct on Age-Appropriate Design (i.e., BIK Code) (2022)

In addition to the DSA, the European Commission develops a range of measures to help protect children online. Better Internet for Kids (BIK) Code is adopted to improve age-appropriate digital services and to ensure that every child is protected, empowered and respected online. The commission encourages and facilitates a comprehensive EU code of conduct on age-appropriate design, covering topics including age assurance, data protection, and clear and accessible information. They also support the development of an EU-wide digital proof of age [58], [59].

D. California Age-Appropriate Design Code (2022)

The Code prompts companies to consider the privacy and protection of children in the design of digital products and services that are accessible to children in California. The requirements include age group considerations for development, data privacy restrictions, age assurance and achieving the highest level of data minimization and default privacy settings [60], [61].

E. Children and Teens' Online Privacy Protection Act (COPPA) 2.0 (2023)

COPPA 2.0 amends the Act of 1998 to strengthen protections related to the online collection, use and disclosure of personal information of children and minors up to age 16 (up from age 13 in the previous version). It also empowers teens to make decisions for themselves by recognizing their growing autonomy and asking for consent before data collection while strengthening special protections for younger children by flatly prohibiting behavioural and targeted marketing [62], [63].

F. Kids Online Safety Act (KOSA) (2022)

KOSA provides kids and parents with the tools, safeguards and transparency they need to protect against threats to children's health and well-being online. It requires online platforms to put the interests of minors under 16 years old first, providing a safe environment by default by creating a duty to prevent specific dangers to minors including promotion of suicide, eating disorders, substance abuse, sexual exploitation or advertisements for certain products etc. As for the parental tools required by social network platforms, default control to the strongest option to best protect minors is required. The Act requires that parental controls should include the ability to control children's privacy and account settings, restrict purchases and financial transactions by a minor, and track time spent on a platform. The legislation also requires large social media platforms to perform an annual audit to assess the risks to minors [64], [65].

G. Utah Law on Social Media Minors (2024)

This law requires social media companies to verify the age of an adult to open/maintain an account, get consent of parents for users under 18, allow parents full access to their children's account, create a curfew for minor accounts, protect minor accounts from

unapproved messaging, and block minor accounts from search results. In addition, the social media companies cannot collect a minor's data, and cannot target minors for advertising or addictive design and features [12].

H. Online Safety Act of the UK (2023)

The Online Safety Act takes a zero-tolerance approach to protecting children from online harm while empowering adults with more choices over what they see online. The act requires companies to prevent and remove illegal harmful content and age-inappropriate content for children. It also requires age verification and reporting functions on platforms kids access [66].

I. Online Safety Act of Australia (2022)

The Act requires industry to shield children from age-inappropriate content and to provide parental control tools for parents [67].

J. Bill S-210: An Act to Restrict Young Persons' Online Access to Sexually Explicit Material, Canada (2023)

The Bill, which remains before Parliament, is intended to keep Canadian children safe online by preventing companies from making sexually explicit material available to them by requiring websites with adult material to have robust age verification mechanisms [68].

Throughout this thesis, when we speak broadly of policy (or policies), we intend to refer to the full gamut of government statutes, regulations, codes of conduct, policies, etc., of the sort listed above, that may be put in place to safeguard and empower children in the digital world.

These new policies can introduce a dilemma in how to verify children's ages in a secure and private way, to discern inappropriate content for different age groups, and to get parents' consent on certain features in the current Internet world. GDPR has been in place for several years, and many controls have been implemented for data protection, but the technological solutions for children's privacy still seem inadequate [30], [69]. Crepax et al. [31] found that most controls put in place do not authenticate properly and identify age groups for minors, causing age-related threats. They suggested that the contents and services accessed by children need to be tailored to rights and interests dependent on the children's precise age for data processing, the developers should be aware of special considerations when it comes to children as they may affect developers' legal obligations, principles of data processing, and most importantly, affects the children. They called for a design based on secure and privacy-friendly technical controls for age identifications targeting children for their age groups, and a need to design tools for accessing children's competence to consent to help enforce privacy regulations with respect to children. Most children and parents believe that age verification would delay the age at which young people first see pornography by stopping them from accidentally stumbling across explicit content at a young age through searches, pop-ups or links sent on social networks [10].

The new policies bring debates and confusion for many reasons (e.g., adverse effects, ineffectiveness, vagueness) [70]. There are debates around parental consent and age verification requirements (e.g., privacy concerns, concerns with respect to freedom and costs associated with blocking websites) [71], [72], [73], [74].

How children's ages would be verified without sacrificing privacy under the new measures and legislation poses a challenge as they require platforms to verify the users' ages in order to hide or block inappropriate content. Some worry that the regulations themselves could cause the

companies to collect more data from minors or restrict access to information. Clear guidance is necessary to guide the companies in their design decisions. Age verification or assurance tools require users to upload identity verification documentation or biometric information and there is currently no sufficiently reliable method that protects individuals' data, privacy and security.

This section identified the gaps in existing parental mediation tools, web content and policies. They are summarized as follows:

- Policies require age-appropriate web content design (privacy protection) and age verification.
- Mediation tools that the content providers and service providers provide work but they do not protect children's privacy.
- There are few clear guidelines to help define what age-appropriate content actually is.
- Few effective or consistent age-verification mechanisms work for children without privacy risks.

Determining what age-appropriate content for different age groups are and the development of parental consent mechanisms are both out of scope in this thesis. Our proposed system tries to reduce the gaps identified above in implementing the age verification and parental control tool in a private and consistent measure.

2.1.2.4 Age-appropriate Content and Ratings

This section discusses existing governance and provides a brief history around age-appropriate content and ratings on various media types.

A. *Movies*

Most countries have their own governance systems to classify feature films either played in theatres or at home. The Motion Pictures Association (MPA) has been rating films to provide parents with the information needed to determine whether a film is appropriate for their children since 1968. The MPA has several operations globally [75], [76].

B. *Games*

The Entertainment Software Rating Board (ESRB) has been rating games either boxed or online since 1994. It has seven different rating categories to suggest age appropriateness, nine content descriptors to indicate either interests or concerns with content, and five interactive elements to highlight online features. ESRB assigns the ratings to digital games using a process developed by the International Age Rating Coalition (IARC) [77], [78].

C. *Mobile apps*

Many countries and device companies have developed their own rating systems on online app stores. Mobile app stores such as the *Apple Store*, *Google Play*, and the *Amazon App Store* have their own rating systems by age group.

D. *Internet content*

There are currently no established age ratings for Internet content.

The Internet Content Rating Association (ICRA) tried a system where users were required to install content filtering software to censor types of content but the system did not gain widespread acceptance [79], [80].

Age-appropriate labels on websites were tried in the EU which required the use of an xml file in the root of every website to verify the age ratings of contents. Parents had to

install an app to act on the label when children accessed websites. They asked webmasters to install the XML file containing the age ratings but the project stalled. How and why the project stalled are unclear. We have not yet received a response to an email asking about the project's result [81], [82].

2.1.3 Design Consideration

2.1.3.1 Usability Design

A. Promote children's online opportunities

As children interact with digital devices like toys, these devices become very natural to them. They often possess far more knowledge than their parents on digital technologies. Wang et al. [83] emphasized that today's children need to be supported for their experience in play and exploration rather than instructed as the studies recommend a shift from parent/teacher-led to a children-centered approach in this domain. They studied the existing literature on children's autonomy-supportive design and categorized it as bolstering children's autonomy in three ways [83]:

(1) as *developing intrinsic motivation and self-regulation*;

(2) *as supporting the ability to make critical thinking and informed decisions*; and

(3) as building *computational thinking and literacy*.

Their further analysis underscored five autonomy mechanisms and 12 design mechanisms that were used by the literature they looked at (See Table 2.2). The five autonomy mechanisms are:

- *Scaffolding:*

  Giving children support when they need it and helping them move through their gaps of knowledge.

- *Decomposing*:

  Break down somewhat complicated digital concepts into entities that are more approachable for children, and advocates child-centered discovery learning where children use what they already know, to acquire more knowledge.

- *Peer support*:

  Encouraging social interaction between children and their peers in order to promote their digital autonomy.

- *Digital playground*:

  Encouraging children to freely interact with digital systems in more embodied ways, and learning through playing.

- *Nudging*:

  Imposing subtle design changes that could alter children's behaviours and reinforce positive ones.

Finally, they suggested that future designs should consider 1) identifying critical points of intervention such as how to maximize influence by using the design mechanisms, 2) putting more emphasis on promoting self-generated knowledge in children, enabling them to think critically on issues, 3) considering translating short-term boosts into longitudinal benefits to promote learning or behavioural changes, 4) differentiation and personalization considering children's diverse needs and backgrounds, and 5) ensuring the prototype allows a low floor,

high ceiling for children allowing more flexibility and providing room for children to grow and explore (e.g., scaffolding for older children and decomposing and nudging for younger children).

Table 2.2 Wang's autonomy mechanisms and design mechanisms for children

Autonomy Mechanism	Design Mechanism	Description/Examples
Scaffolding	just-in-time prompt	Give children "the support just when they need it" through introducing information and help buttons.
	informative interaction	Children's interactions and communication between their tutors, parents or even the technological prototype.
	scaffold choice of own	Children to become more aware and more responsible for their own activities online.
Decomposing	storytelling	Support children to construct stories about digital concepts (e.g., elements of algorithm) based on concepts that they are familiar with.
	gamification	Breaking down digital concepts into game elements that children are more familiar with. Help children become familiar with digital concepts through game playing.
Peer Support	peer collaboration	Encourage children to work together to solve problems, complete tasks, or learn new concepts.
	peer comparison	Encourage children to compare their works/performance with others to support their development.

Autonomy Mechanism	Design Mechanism	Description/Examples
Digital Playground	digital playground	Support children to freely explorer and interact with the physical artifacts around them, supporting through more embodied movement and activities.
Nudging	default options	Setting user's pre-set goals as default options. These preset goals include online/offline time, content they want to see etc.
	creating frictions	Use of extra activities or tasks to pause children's immediate next step.
	fear alert	Use of fear messages to stop children - take protective measures or to refrain from activities that might harm themselves or others.
	social feedback	Attempt to alter children's behaviour based on the feedback or comment from others.

Badillo-Urquiola et al. [84] studied how children conceptualize stranger danger online from co-design sessions with children aged 7-11 years and recommended design considerations. Children wanted the app rather than parents to provide assistance as they wanted privacy. Children did not like being monitored out of fear parents may misinterpret the situation, overreact and blame them, but they still wanted help. The recommendations follow:

1) Design automated intelligent assistance.

2) Design should notify children and parents about potential dangers and bad actors.

3) The sites should provide scaffolding that supports children and encourages dialogue and learning opportunities about how to mitigate online risks.

Nouwen et al. [33] studied how digital tools can stimulate interaction between parents and children to support online opportunities and suggested the design solution should offer prolonged negotiations, and try to enrich data on children's online activities by providing families with clues on how to engage with each other in their online activities.

B. Children friendly design

Twenty-five parental control tools for computers and mobiles were tested and benchmarked in a study done by the European Commission [27] to gauge their effectiveness for age groups, usability and security. The study found that none sent alert messages to children or teens, but rather to adults. Some tools redirect to safe resources or allow children to ask for unblocking.

C. Flexible design to consider family context

Mazmanian et al. [44] found that current parenting tools focus on restriction and control but they should be more ubiquitous and allow for broader family dynamics and circumstances such as when children do homework or learn new skills. Kalinowski et al. [24] studied factors that affect content choices for children, parental attitudes towards screens, and devices used. They recommended that designs should consider siblings, and preschoolers (literacy) as predictors of child use. Shin et al. [49] recommended the design to provide communication triggers for the families and to support the transactional nature of family dynamics over time.

2.1.3.2 Features

Common features of the existing parental mediation tools are as follows [5], [26], [27]:

A. *Rule settings*

- Browse control or web content filtering:

  This feature enables parents to control what sites can be accessed with different prevention methods such as allow/block lists. Keyword filtering is uncommon. Many tools have an option to block access to social networks and some include an option to force the user to use safe search functionality which provides only limited protection when searching online.

- Application blocking:

  It allows to block certain applications.

- Time control:

  This feature limits the time or hours when children can connect to the Internet.

- Content control:

  Many tools filter web content by topic. It enables access to the sites or applications appropriate for children.

B. *Monitoring*:

  Most of the tools have a feature to provide the parent with at least a basic report on the user's web activity (visited websites, violations or time spent). The monitoring features allow parents to supervise the websites and time children access.

This thesis incorporates the common features and design considerations from this section.

2.2 Value Sensitive Design (VSD)

2.2.1 Conceptual Investigations

VSD [35], [36] takes questions of *who* the direct/indirect stakeholders affected by the design are, *what values* are implicated, and *how* we can engage the trade-offs among the competing values in the design, implementation and use of the information systems, and *weighing* between moral values and non-moral values. Careful working conceptualizations of specific values often clarify the fundamental issues raised by the project, providing a basis for comparing results.

In the conceptual investigation, direct and indirect stakeholders affected by the technology are identified, followed by an analysis of how these could be harmed by or benefit from the technology. Additionally, the values implicated by the use of technology are identified and defined.

2.2.2 Empirical Investigations

Empirical investigations applied to human activities are observed, measured and documented.

Under empirical investigations, quantitative and qualitative methods are employed to evaluate how stakeholders experience technology with regard to the values they consider important, and they focus on research questions.

2.2.3 Technical Investigations

VSD adopts the position that technologies in general, and information and computer technologies in particular, provide value suitability from their technical properties. The aim of the technical investigation is to combine insights from the other investigations and explore how technology can be designed to support the values identified.

This thesis uses the lens of the VSD approach with the values from the TOSS framework plus privacy and content control by age groups in conceptualizing, implementing and evaluating the proposed system with the goal of enhancing the security and privacy of children online.

2.3 Privacy

Restricting what you give away is easier

than restricting what is taken from you. – Carlisle Adams

This section opens discussions about the ever-vague subject, of what information privacy is about, and considers recommended privacy design approaches.

2.3.1 Definition of Information Privacy

Personal information is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual [85].

Westin [86] defined privacy as an entity's ability to control how, when and to what extent personal information about it is communicated to others.

Information privacy is defined by Solove [87] as not only about controlling immediate access to oneself but also about reducing the risk that personal information may be used in an unwanted way suggesting two distinct dimensions in access control and risk management in building privacy-friendly technology and information systems [18].

2.3.2 Privacy Attitudes

People have different attitudes and perceptions towards privacy (or security) depending on their experience, education and socio-economic background. Studies have found that some users do not really understand privacy and security, and this results in passive behaviours of preferring convenience over privacy [88], [89]. People are unconcerned about privacy until they are breached [18], [20]. However, people have had legitimate concerns about individual privacy and Smith et al. identified seven dimensions of what people are concerned about [17], [90]:

1. *collection* and storage of extensive amounts of personal data,
2. *unauthorized secondary use by the collecting organization* for different purposes than the ones users have authorized,
3. *unauthorized secondary use by an external organization* with whom personal data has been shared,
4. *improper access* to personal data, e.g., identity theft
5. *errors* in personal data that can happen deliberately or accidentally become stubborn, erroneous problems as well as reluctance to delete old data,
6. *poor judgment* through decisions made via automated formulas or rules in companies, and
7. *combining data* from disparate databases to create a combined and more comprehensive profile.

Despite the privacy concerns, people do not act according to their preferences as they claim to do. At the same time, much existing online privacy behaviour simply goes unobserved leading

to false conclusions that people do not care. Privacy is actually an issue for the majority of people even though they engage in data-intensive services and do not protect their personal data sufficiently. Also, developers providing technological tools and digital content do not understand the purposes and requirements of the privacy aspects of their projects [91], [92]. Education efforts, technical recommendations, and public policy recommendations are becoming crucial to enhancing users' privacy and security [19], [93]. Recent studies suggest that new privacy regulations are increasing public awareness of privacy. More consumers pay a premium to shop at websites with good privacy policies when privacy information is readily available in search results.

2.3.3 Children's Privacy

Young children do not understand privacy very well [94]. They may unintentionally click on any button of pop-ups or messages that appear while they are going about their digital activities. There are growing concerns about generic controls aimed at protecting children's privacy proving insufficient to protect children's privacy as children are getting better at circumventing age verification mechanisms, using adult devices to access inappropriate content, or consenting to privacy policies they do not understand. There is no technical standard or best practice providing controls that are specifically designed to protect the privacy of children [31].

Crepax et al. [31] studied control tools designed for children's privacy and grouped them into four domains which are social media (e.g., online grooming[3], sharenting[4], or children posting themselves which they will regret in the future, targeted advertisements, profiling), surveillance (e.g., surveillance smart devices, CCTV, drones with cameras etc.), domotics (i.e., home

[3] See Glossary for online grooming.
[4] See Glossary for sharenting.

automation) and educational software. Note that children do not have a choice not to use the educational software used in schools.

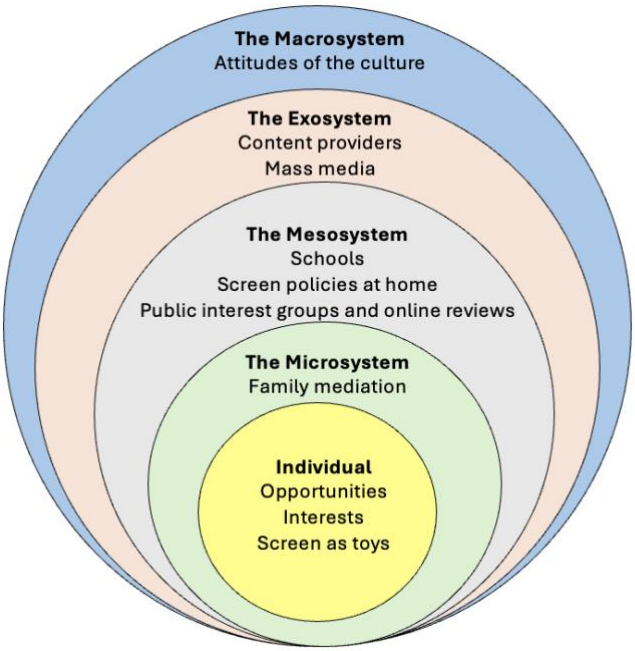


Figure 2.2 Ecological context of children's selection of media context inspired by Bronfenbrenner

Teachers and schools play a key role in educating children about digital security and privacy as well. Teachers and parents need to work together on educating children on the proper usage of digital tools and schools should provide adequate training to teachers on security and privacy [23], [95]. Kumar et al. [25] conducted a study on privacy and security considerations in school learning and found that educators consider digital privacy and security as it relates to handling student data and minimizing inappropriate technology use. They said students rarely received lessons focused on privacy or security. They considered their findings through the lens of ecological framework of Bronfenbrenner [96] through which they can see the learning as it occurs in microsystems, mesosystems, exosystems, macrosystems and chronosystems (see Figure 2.2).

They suggested schools 1) integrate privacy and security features and lessons into classroom technology (e.g., by incorporating privacy and security features that meet educators' need, and by designing technology that highlights teachable materials related to privacy and security), 2) incorporate digital privacy and security lessons across the school and home context, (e.g., mobile apps should embed various privacy resources on their websites and suggest ways for educators and parents to discuss them with children), 3) improve educators' knowledge about digital privacy and security (e.g., develop and disseminate resources that help educators understand and evaluate digital privacy and security concerns and incorporate privacy and security into efforts to build technological pedagogical content knowledge (TPCK) and 4) address tensions related to the datafication of education (e.g., Will companies like Google delete data from their educational platforms when children move to the next grade?).

Zhao et al. [94] studied children's (age 6-10) knowledge about privacy risks and how their behaviour changed after adopting coping strategies. They showed that even young children, just like adolescents and adults, like to have their privacy respected after learning how personal data can be collected and used via mechanisms like data tracking or in-app recommendations. They showed recognition of privacy risks after learning but did not always take effective action as people react to situations using their current knowledge and experience. Their study demonstrates the importance of educating children about privacy risks and coping strategies at a young age.

2.3.4 Risks

We look at privacy risks that can happen by using technologies in this section.

Users are concerned about the collection and storage of extensive amounts of personal data and unauthorized secondary use by collecting organizations and external organizations. Their concerns arise from undesirable data usage once data has been collected and is no longer under

the user's control. Spiekermann and Cranor [18] discussed privacy spheres and system activities which can impact user privacy.

A. By Privacy Sphere

1. User sphere:

   This encompasses a user's device. Data should not flow in and out of these devices without their owners being able to intervene.

2. Recipient sphere:

   This is a company-centric sphere of data control that involves backend infrastructure and data-sharing networks. There is the risk of potential privacy breaches due to data leakage and uncontrolled or undocumented access and sharing practices.

3. Joint sphere:

   This encompasses companies that host people's data and provide (often free of charge) additional services (e.g., email). Users expect 'privacy' when they use these services, but these services are under the full control of the companies providing them. There is the risk of personal data abuse without careful privacy design with proper access control and security mechanisms.

B. By System Activity

1. Data transfer

   - Data transfer from a user's system to a service provider:

     Involves explicit user involvement (e.g., fill out a web form), and explicit data transfer without user involvement (e.g., web browser cookie, camera recording

etc.). The latter form of inappropriate, uncontrolled transfer raises greater privacy concerns.

- Data shared within their own organization and to external third parties:

  Privacy leakage is a concern when data is transferred within the joint and recipient spheres in an inappropriate or uncontrolled way without transparency in policy communication. The joint spheres are sensitive as users tend to believe their online data should not be available to any third party.

2. Data storage

   - Local devices:

     It is a privacy concern when local applications store data on a user's personal system without letting the user know. Privacy breaches occur when users, unaware of such client-side storage, have their activities discovered by others.

   - Persistent vs. transient storage:

     Persistent storage involves data stored indefinitely or over multiple transactions accumulated and retrieved at a later time. Transient data storage has minimal privacy implications while persistent data storage can raise significant privacy concerns.

3. Data processing

   Data processing refers to any use or transformation of data typically done outside the user sphere.

- Secondary data use:

  Companies often engage in secondary use of personal data that is not expected by users. For example, companies may group customers into segments based on their purchases or scan their emails to market personalized services. Also, data processing may be outsourced to a third-party service provider, raising additional privacy concerns. There is a growing list of privacy breaches and identity theft incidents that have occurred due to negligence on the part of third-party service providers.

2.3.5 Privacy Design Approaches

As with security, privacy must be protected right from top to bottom. Privacy requirements must be addressed throughout the full system development process and privacy protection cannot be implemented as a single layer or by installing a single app [38], [39].

Privacy is protected by limiting the exposure of operations and disclosure of records by hiding identity, attributes and actions [39]. A privacy design is a design strategy that achieves some level of privacy protection as its goal. Design strategies are applicable during the concept development and analysis phase of the development cycle [38].

Adams [39] suggested a roadmap to individuals' privacy protection as follows:

A. Make some decisions

1. Decide what your privacy is worth to you.
2. Decide what amount of privacy we want to achieve and what we are willing to do to attain that level of privacy.

B. Take some actions

1. Become knowledgeable about your data.
2. Become knowledgeable about the potential risks.
3. Take explicit steps to guard your personal data. Restrain yourself in the personal data you give away so that your future is less at risk.
4. Constrain what you unintentionally give away in terms of data. Assert authority when dealing with other entities. Refuse to share what does not need to be shared.

Hoepman [38] suggested privacy design strategies for technical controls with data protection by design and by default. The strategies were derived from existing privacy principles and laws on which the designs of an IT system have a potential impact. The derived privacy design strategies include *data-oriented* strategies and *process-oriented* strategies. Table 2.3 shows the data-oriented strategies. This thesis only mentions the *data-oriented* strategies as the *process-oriented* strategies apply to organizations processing data. The *data-oriented privacy* design strategies correspond to the *privacy-by-architecture* approach identified by Spiekermann and Cranor [18].

Table 2.3 Data-Oriented Strategies

Strategy	**Description**	**Application**
MINIMIZE	The amount of personal data that is processed should be restricted to the minimal amount possible.	*Select before you collect, anonymization* and *use pseudonyms*

HIDE	Any personal data, and their relationships, should be hidden from plain view. It aims to achieve *unlinkability* and *unobservability*.	*Encryption of data*, *mix networks* to hide patterns, *attribute-based credentials* to unlink certain related events, *anonymization*, and the *use of pseudonyms.*
SEPARATE	Personal data should be processed in a distributed fashion, in a separate compartment whenever possible.	This calls for distributed processing instead of a centralized solution. Data from separate sources should be processed locally whenever possible, stored locally if feasible. Database table should be split whenever possible, and rows should be hard to link to each other. Centralized service platforms like Facebook and Google lacks this.
AGGREGATE	Personal data should be processed the highest level of aggregation and with the least possible detail in which it is still useful.	*Aggregation over time* (e.g., used in smart grids), *dynamic location granularity* (e.g., used in location-based services), and *k-anonymity* [97].

Spiekermann and Cranor [18] proposed a methodology for systemically engineering privacy friendliness as the *privacy-by-architecture* approach. They argued that engineers can make architectural choices on two distinct dimensions, network centricity and identifiability of data. Systems developed offering more client-centric architecture provide higher levels of privacy friendliness than systems that collect personally identifiable data. Applications with client-centric architectures minimize the need for personal information to leave the user sphere. (See Figure 2.3).

1. Network vs. client-centric architecture

   More network centricity means potentially less privacy for clients. The more network-centric a system is, the more the network operator knows about the client and the more he can control the client.

2. Use identifiability

   The more personally identifiable data that exists about a person, the less she is able to control access to information about herself, and the greater the risk of unauthorized use, disclosure, or exposure of her personal data.

   The ability to link personal information to create a comprehensive profile is the key to determining the degree of privacy a person has. Linkage can occur directly by joining database information or it can be achieved indirectly by pattern matching.

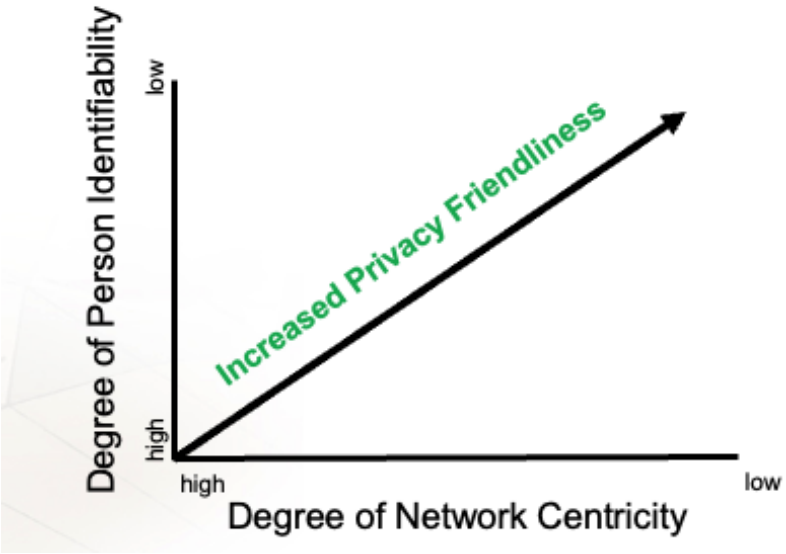


Figure 2.3 Privacy friendliness of architectural choices

In their study [18], Spiekermann and Cranor mention an important concept around *reidentification*. Many service providers offer users pseudonymous self-representations knowing that privacy concerns can be reduced in a network-centric system if data is not stored in an identifiable form as a unique individual. However, pseudonyms do not automatically provide privacy-by-architecture. Pseudonymous profiles can be reidentified by linking them with identity information stored in another database within the same company or by employing data mining techniques on pseudonymous transaction logs. They also introduced a degree of identifiability to measure the privacy of design and recommended measures to reduce the risk of profile linkage and pattern matching. Privacy-by-architecture does not guarantee unlinkability, but it ensures that the process of linking a pseudonym to an individual will require an extremely large effort.

2.4 X.509 Certificate

2.4.1 Certificate Management, Distribution and Revocation

Public-key infrastructure (PKI) for the Internet web handles the key management, distribution and revocation in an isolated hierarchy as a chain of trust and enables web browsers to authenticate web servers by verifying the X.509 certificates belonging to one of the trusted roots. X.509 certificates are then used for encryption once verified as a trusted source as part of Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols.

The X.509 authentication framework was designed by International Telecommunication Union (ITU) to work with a hierarchy of certification authorities (CAs). X.509v3 published in 2008 is a current general-purpose public key certificate for the Internet. The format of the X.509 certificate is illustrated in Figure 2.4.

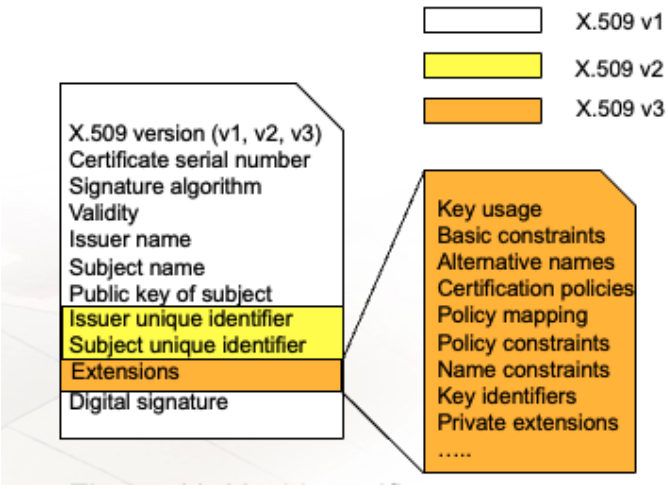


Figure 2.4 X.509 certificate format including extensions

The certificates can be revoked if they become invalid for some reason. The revoked certificates are managed in a Certificate Revocation List (CRL) of a CA.

2.4.2 Certificate Validation in Web Browser

94% of total website connection requests on desktop services and 93% on mobile devices use Hypertext Transfer Protocol Secure (HTTPS) while 89% of website home pages are served up on desktop devices via HTTPS and 85.5% for mobile site home pages [98].

Secure web communication using the Transport Layer Security (TLS) protocol depends on both trustworthy certificate issuance and management procedures and reliable certificate validation mechanisms [99].

For the validation procedure, a user must obtain the root public key of every PKI in order to validate the certificates of users in the chain of trust of all hierarchies. Users belonging to hierarchies with an unknown root cannot be identified. Most popular web browsers are equipped with about 50 of X.509 root public keys in their trust stores.

In short, the browsers with TLS/SSL implementation check the authenticity and trust of the certificate before displaying the content to the user. Certificate validation is implemented by a web browser on behalf of the user to determine whether or not to trust a presented certificate before building a secure communication channel and loading the content in the browser. The validation includes checking field values, identity, chain validity, key usage and revocation as shown in Figure 2.5.

The limitations of web browsers in validating X.509 certificates exist in inconsistent manners seemingly due to complex and vague standards, and a lack of coordination between

browser suppliers [100]. Mobile web browsers are also known to be weak in the certificate validation [99].

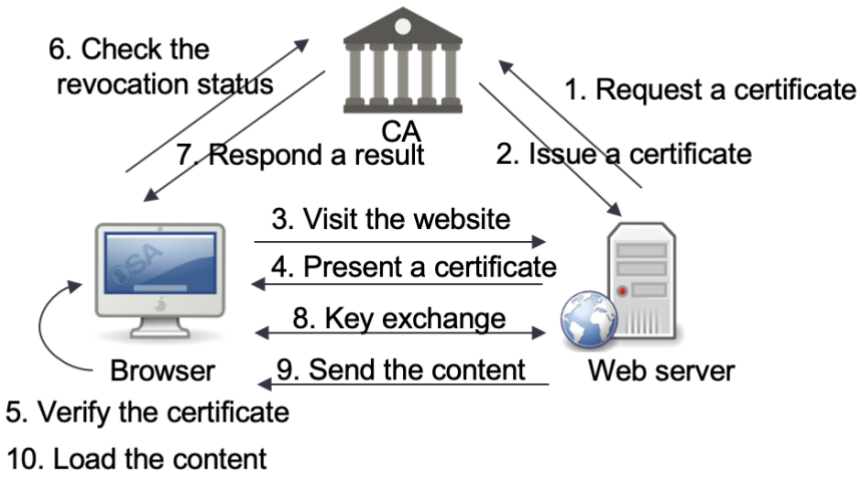


Figure 2.5 Illustration of the Web PKI inspired by Luo et al.

2.4.3 Certificate Extensions

The X.509 certificate provides various basic and extension fields for defining a certificate. The optional extensions allow additional policy information to be included which can be either critical or non-critical. The extensions provide methods for associating additional attributes with users or public keys and for managing relationships between CAs [102].

Browsers can ignore invalid or unrecognized non-critical extensions, but they are required to process and validate all critical ones [101].

Each extension carries information associated with an Object Identifier (OID) which is a unique number of positive integers used to distinguish objects and an ASN.1 structure.

Applications such as browsers are expected to have their own policy OIDs to be able to map the extensions [103].

Our proposed system utilizes this extension field to associate an age rating of the website to the certificate. The optional field was used as a proof of concept only, but it should optimally be a required field for the system to operate with a reasonable size of network implementing it.

2.5 Related Work

The number of studies on parenting mediation tools is growing rapidly. This section looks at existing work related to designing tools for online child safety.

A. Parenting Mediation Tools

Ko, Minsam et al. [26] studied how participatory parental mediation for teens can overcome restrictive approaches. They reported restrictive functions such as remote monitoring, filtering, and blocking were limited for teens due to their intrusiveness, and they developed *FamiLync* app in which they consider limiting the use as a family activity where each member self-monitors their own usage and tries to self-regulate their usage. The study results showed that the family members better understood their usage patterns with *FamiLync*'s self-monitoring support. It improved mutual understanding of usage patterns and facilitated discussions between family members while reducing smartphone usage amounts and improving parent-child interaction. The study was successful in improving the value of self-regulation, but the parental mediation app had time usage monitoring and restriction features only and targeted teens.

Ghosh, A.K. et al. [104] designed an Android application called *Circle of Trust* by which parents and teens could co-mediate text messaging and negotiate trusted and non-trusted contacts and conducted an initial exploratory user study with parent-child pairs for its usefulness, ease of use and behaviour intent to use. For teens' privacy, the parents only saw risk-flagged content and message summaries using results employing the theoretical lens of VSD, valuing the child's privacy, trust, and freedom and balancing the needs of both parents and teens. The study evaluated the app with an initial exploratory user study and participants found the app less invasive and beneficial for parent-child relationships. The app provided features satisfying all TOSS strategies but was better suited for teens, not young children as it provided a text message monitoring feature only.

McNally et al. [48] held multiple design sessions with children aged 7-12 years old to redesign an existing parental monitoring/restricting tool called *TeenSafe*. They also surveyed children about their age, mobile use, current monitoring strategies and effects and their effectiveness. The study proved that children in this age group accepted some monitoring of where they are and the history of where they visited, especially those incidents with 'bad word' posts. The children had a desire for privacy after a design session by education. Their design recommendation based on children's desires was to add more interactions on parental mediation tools such as immediate incident management assistance or showing disapproval buttons on harsh messages sent. The tool was for mobile use only and was not conceptualized technically. However, the re-design sessions introduced new features such as requesting and approving URL lists between children and parents, and immediate incident management assistance thereby

extending active mediation and self-coping strategies in line with TOSS values. The study proved that TOSS values also apply to young children.

Sangal et al. [45] proposed a self-regulation tool as an app *Teen-Alyse* whose values extend TOSS and feature teen regulations in self-monitoring and active mediation values. They viewed the control of monitoring and restriction makes the parental style quite passive and authoritarian, but it helps the parents to observe and restrict the teen's activities and help the teen if the risk increases or the teen is undergoing some online threat. The application has a self-monitoring feature for teens, flags URL reports for parents and enables parent-teen active mediation. The app was developed to improve self-regulation habits for teens. The application flagged URLs by comparing content names to the stored flagged content words which are likely to produce inconsistent results.

Yadav et al. [51] developed a mobile application that detects inappropriate content accessed by children and provides monitoring reports to parents. They held an initial exploratory user study with children aged between 4 and 10 years old and their parents. Their findings about children's behaviour and analysis are shown in Table 2.1. The result analysis found that young children were found watching violent content while randomly clicking and accessing random pop-up links. They preferred to access violent graphics than violent text and the frequency of visiting violent content grew as they became older. They emphasized parents' awareness about the online activities of their children to properly guide and counsel them. The tool monitored all activities of the children, and they were provided in the reports to the parents which could be considered a privacy violation.

B. Machine-Learning(ML) Based Tools

ML-based parenting mediation tools provide a restriction feature allowing for the filtering of content based on restricted words or website URLs by crawling the content and using ML algorithms to learn keywords and websites.

Kuma et al. [105] built a browser-based mobile parental control tool to filter contents using an ML-based approach to classify websites to block inappropriate content and provide parents with features to control and monitor their children's online activities, and to help mitigate the risk of cyber threats for children. The ML feature focused on parental restriction, but an extra layer of design was added to communicate between parents and children about wrongly blocked URLs. Fuertes et al. [106] developed a tool detecting and blocking websites with inappropriate content by filtering keywords learned by Natural Language Processing (NLP). They recorded children's activities and analyzed their online activities. But the results did not show how successful their NLP algorithms were in blocking the intended sites. The findings from surveys of teens, parents and school technicians identified online safety measures used, and the risks teens face which revealed that parents did not know how to mediate their children online while teens accessed the Internet freely. Lack of knowledge of mediation tools and technical issues were the reasons.

The tools in this section provided features limited to certain age groups only. They focused on a subset of TOSS strategies and proved they worked well. However, none of them provided age-differentiated features targeting children of all ages up to age 18 years old. They either flagged or blocked harmful content by using filtering algorithms which may have unexpected results and the methods are not age-differentiated. Our proposed system tries to balance the three

mediation styles and some of the teen self-regulation strategies from the TOSS framework while adding privacy and age ratings. This thesis also considers five different age groups with differentiation between young children and older children above 10 years of age.

2.6 Chapter Summary

In this chapter, we discussed how existing literature conceptualizes parental mediation tools, and a design approach employing VSD, and information privacy.

The recommended parenting mediation strategies along with teen strategies are defined using the TOSS framework, a combination of them can promote children's safety and autonomy. The key is to balance all the strategies as children grow while allowing flexibility depending on the family context. While various mediation tools are available to help parents support children (although they are mainly restricting or monitoring), many parents are still skeptical on using them for various reasons such as technological issues, usability or other. Studies show that there is no single tool that works well for everything, and they are weak in security and privacy. One of the recommended design approaches for mediation tools is to differentiate age groups for children so that they can support children's growth as they change behaviours and prevent harms, meaning that the tools should support the balancing of the parenting strategies and teen strategies mentioned above.

We went on to discuss how governments and industry are participating in age-appropriate design to support children in digital environments. Many policies and laws have been introduced and enacted globally starting with GDPR in 2018. Since then, the industry has made efforts to introduce mechanisms designed to protect minors, but they are still inadequate. Furthermore,

debates exist for proper age-verification requirements derived from the policies. The age-verification requirements are about adult content, but some studies suggest that children also need to age-verify to mitigate harmful content. Obviously, all the key stakeholders in the children's digital ecosystem are trying their best to support children on their own (with their own knowledge and experience, but some for their own profits as well) but there are gaps in between.

The history of age rating systems of other media content was discussed in brief. Proper governance and regulations have been established for movies and games historically.

Usability design guidelines for tools children access and parenting mediation tools and a design approach VSD were discussed as we designed a parenting mediation tool with values for children. Supporting their autonomy, offering children-friendly design, and considering family dynamics while keeping them safe are important usability considerations when designing parental mediation tools. Rule settings such as time and content restrictions and monitoring were the most common features of existing parenting mediation tools. VSD is a theoretical design approach which helps integrate human values into technological solutions by considering key stakeholders affected by the design and iterating conceptual investigations, empirical investigations, and technical investigations.

The definition of information privacy by Solove [87] implies two dimensions of privacy risk mitigation approaches such as access control and risk management. People in general, including children, do not understand privacy very well. People's privacy attitudes differ by their background, and they do not always act on or know how to respond to the privacy concerns they might sometimes have. It is important to educate everyone, including children what privacy means in their own environments. The roles of teachers and schools become important here as well as parents. Privacy risks can be identified by analyzing the privacy spheres and system

activities the system is related. The risks exist in all three spheres, the user sphere, the recipient sphere and the joint sphere, but the privacy protection design should be handled with extra care for data in the joint sphere as it encompasses companies that people blindly trust and supply personal information to. For system activities, how data can be discovered by unintended parties was considered in three dimensions including data transfer, data storage, and data processing. Note that *secondary data use* that can happen during the data processing activity is done outside the user sphere. Privacy design approaches recommended by Hoepman, Adams and Spiekermann were presented.

Finally, we looked at how X.509 certificates in PKI structure work with browser applications and extension fields are available to add additional authorization information which is useful for our purpose as will be seen in the next chapter.

We consider the identified gaps (see section 2.1), incorporate the tool design recommendations and privacy design recommendations (see sections 2.1.3 and 2.3.5), and use the lens of VSD integrating values, privacy, age ratings as well as TOSS values in the proposed design of our parenting mediation system in the next chapter.

Chapter 3

Proposed System

This chapter contains the design architecture and implementation details of the proposed system *ProKids.*

3.1 System Design

3.1.1 Privacy Design

This section is organized so that the privacy design of *ProKids* follows the privacy protection roadmap by Adams [39] as those action steps are also applicable in privacy design:

A. *Data associated with parental mediation tools (i.e. become knowledgeable about your data)*

- *Parents' identification*:

  Most mediation tools require parents to set up their profiles first for accounting purposes. This step requires parents to enter personal information from email addresses to complete the user profile including contact information.

- *Children's identification*:

  Some parental mediation tools require only a pseudonym (e.g., *Netflix Kids*), but sometimes they require personal information such as birthdays and/or email addresses. Note that even if they are pseudonyms only, reidentification or linkage can occur by combining them with parents' identification or other databases available to the company.

- *Children's online activity pattern*:

  Most parental mediation tools provide a monitoring feature that tracks children's online activities and a reporting feature that provides parents with such a report. Often parents' email address is required to receive a monitoring report.

- *Rule settings*:

  Other rule-setting information such as allow/block URLs or apps, a browsing schedule, or a purchase limit is entered by parents.

- *Other data:*

  The age-verification mechanism design is out of scope for this thesis but more robust age-verification mechanisms will require vast amounts of personal information such as a driver's license, and biometric information such as speech recognition, facial features or fingerprint characteristics entered into the website. In addition, age verification using biometric information will require the setup of additional hardware [69].

B. Become knowledgeable about the potential risks

We discussed privacy risks for technology use in section 2.3.4 for different privacy spheres and system activities according to where the risks can happen. Of all the privacy spheres, joint spheres are where risks tend to lie for most popular parenting mediation tools (e.g., *Google Family Link*, *Apple Parental Control* and *Microsoft Family Safety*) as the data is often transferred to the joint spheres. Data is often transferred to the joint sphere, stored and processed in the joint sphere which raises greater privacy risks. Many studies found weak security and privacy risks in current parental control tools with improper access control, vulnerable SDKs, and transmitting data in HTTP, not HTTPS

[2], [27], [28], [29]. As for data related to age verification, children can easily bypass most age verification mechanisms implemented now, and be exposed to privacy and security threats [69]. For example, Figure 3.1 shows two age verification apps that can be integrated into Shopify-generated websites in which a user needs to enter a birthday to verify the age or simply agree to a statement [107]. Even the weak mechanisms require birthdays entered into the website, causing data transfer to, data processing in the joint or recipient sphere which raises privacy risks. Cyber threats taxonomy for children including the privacy breach category is also depicted in Figure 1.1.

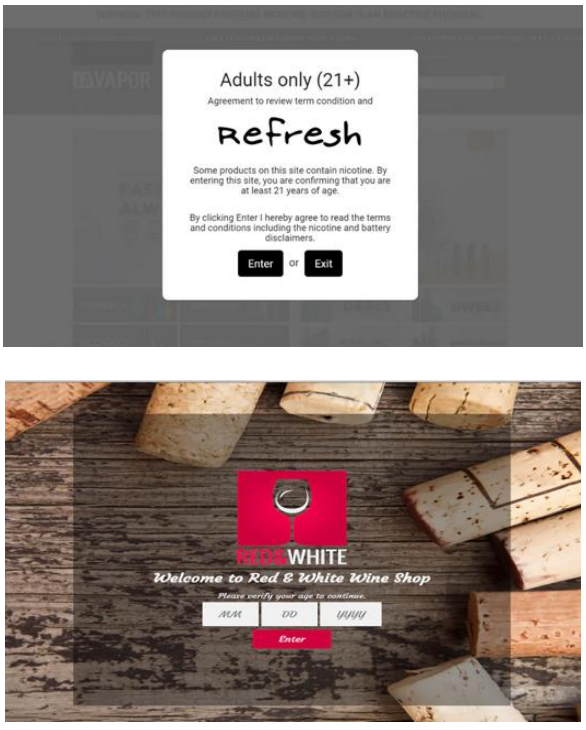


Figure 3.1 Age verification apps

It is important to note that some parental mediation tools may invade children's privacy space by being too invasive. Monitoring certain activities only such as suspicious

activities and transparent communication between parents and children are recommended [2], [94].

C. *Take explicit steps to guard your personal data. Make a habit of restraining yourself in the personal data you give away so that your future is less at risk.*

We continue with the risks discussed above related to user spheres and system activities strategies for achieving privacy in each category in Table 3.1. This table also shows how *ProKids* design follows each privacy design strategy discussed in section 2.3.5.

Table 3.1 Privacy design strategies in ProKids

Strategy		**Application to ProKids**
Privacy Spheres	User sphere	Data should not flow in and out of them without their owners being able to intervene. We store all data described above including user settings and history of children accessing inappropriate sites in the local device (user sphere) only.
	Recipient/Joint sphere	Company-centric sphere of data control that involves backend infrastructure and data sharing networks. Engineers should minimize the risk of potential privacy breaches due to data leakage and uncontrolled or undocumented access and sharing practices. The system is not a company and all information stays in the user sphere, so these recommendations are inapplicable. However, the user profile and history data are password protected for access control and the password is stored encrypted.

System Activities	Data transfer	Most other parental control tools transfer data to the recipient or joint spheres. ProKids does not transfer any data in and out of the user sphere.
	Data storage	Transient data storage has minimal privacy implications. Reset feature for all data including user settings and monitored history of activities to meet the transient data storage requirement.
	Data processing	The sole purpose of getting user's birth year in user profile is to be able to match the age rating of contents. The processing happens in user sphere.
Hoepman's Privacy Design Strategies [38]	MINIMIZE	The user setting collects the minimal information needed to process age rating verification. For user's age, we collect only the birth year omitting the birth day which is identifiable data.
	HIDE	There is no parental information in the user setting, also we use a pseudonymous profile employing a nickname instead of real name so there is no linkability.
	SEPARATE	There is only one user per device for now, so k-anonymity is not feasible.
	AGGREGATE	Verifying the content age rating using a PKI system requires no personal data leaving the device, only the age rating to match the

		extension field of the X.509 certificate. No personal details are used in the data processing.
Design-by-Architecture [18]	Network/Client Centricity	ProKids is client-centric by design.
	Degree of Identifiability	ProKids design meets stage 2 of the *degree of identifiability*, as It is designed for the non-identifiability of users. The birth year is used instead of the precise date of birth. The profile is under a pseudonym.

3.1.2 Design Model

We propose a parental mediation method that allows children to explore the Internet in a safer and more secure way and allows parents to mediate their children by sharing less information about their identities with companies while putting the onus on other stakeholders such as content providers and governance practitioners (e.g., government, regulators etc.) as set out below.

3.1.2.1 Actors

There are four actors participating in the system model.

A. Governance partitioners (government):

These are responsible for implementing policies and actions such as audit requirements and regulations. The system requires governance responsible for rating and validating the ratings for the websites at set intervals. They will also have to communicate the website ratings to the CAs so that they can certify certificates that contain age ratings.

B. *Content providers (industry):*

They are responsible for providing the age rating for their own websites in the TLS/SSL certificates.

C. *Parents/Guardians:*

Parents are responsible for establishing the user settings of the browser for children.

D. *Children:*

Children are the beneficiaries of the system who can thus explore, and learn from, the Internet.

3.1.2.2 Theoretical Design Model

The proposed system incorporates the TOSS strategies as well as privacy and age groups. The features are considered from section 2.1.3.

A. *Privacy*

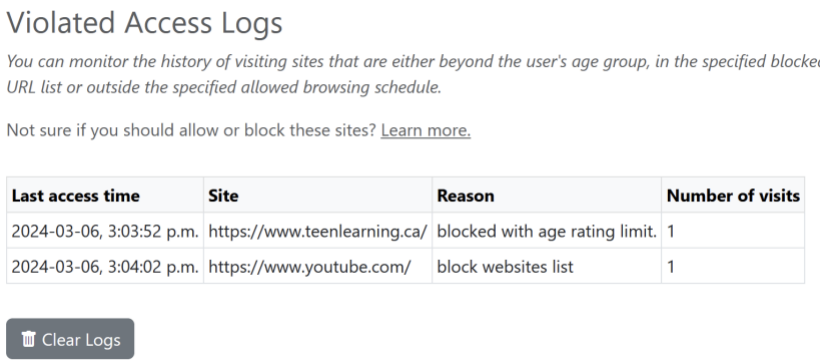
In section 3.1.1, we looked at how the *ProKids* design follows various privacy design strategies. This section looks at each feature to see how privacy design is achieved.

- User settings:

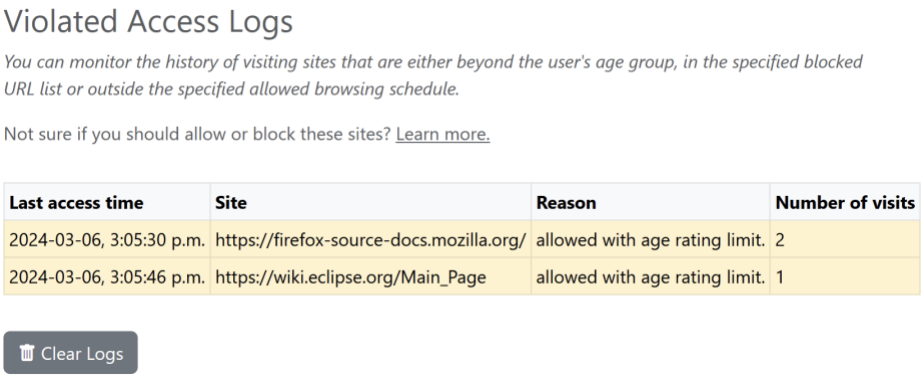
ProKids stores the user settings including user age and the rating in the device only, and the data is not transmitted to the Internet. The implementation is done in a Firefox browser add-on. This was for convenience as a proof of concept. Realistically, we would want this to be a separate application on a device.

- Monitoring report of inappropriate content visits:

The ‘view monitoring report’ feature is shown in Figure 3.2. To protect children’s privacy, only attempted visits to inappropriate content made by younger children and only visits to inappropriate content by older children are recorded and shown to parents. (All visits to inappropriate content, i.e. content with higher age ratings, by younger children are automatically blocked and so there are no such visits to record in this feature.) The history is stored on the device only and can be permanently deleted using the *Clear Logs* button.



(a) Content with higher age ratings is automatically blocked for younger children



(b) Content with higher age ratings is allowed with warnings for older children

Figure 3.2 Violated access logs in ProKids

- Using the X.509 certificate

  The X.509 certificate is used by the web browser to validate the age ratings of the websites children visit before loading the content but after the SSL/TLS handshake. This removes the inconvenience of the website verifying the user's age and children having to give out personal information to the website. Figure 3.3 shows the certificate request with the custom extension field showing the age rating P (for preschool) added as *kidsAssProp* (for kids assigned properties).

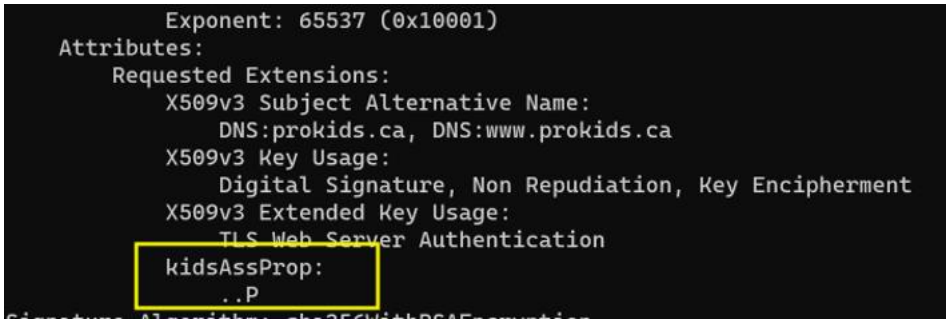


Figure 3.3 X.509 certificate request with custom extension KidsAssProp

B. Age Rating

The system enables children to browse the Internet more freely with a safety net. More safe content with their appropriate age ratings becomes available to younger children. This also helps parents as they do not have to constantly maintain allow/block lists of URLs.

C. Monitoring

A monitoring report of access to blocked or inappropriate content is shown to parents. They remain on the device and are cleared on demand.

D. Restriction

- Content control by age groups:

  The proposed system enables automatic content control for different age groups by using X.509 certificates. This feature should allow a good default list of content for children in different age groups. How to rate the content is out of the scope in this study.

- Time limit:

  The feature allows one to limit the time of day or hours that children are able to browse.

- Content control by list:

  This feature considers different family contexts such as socio-economic backgrounds, family dynamics etc. It adds flexibility to content control by age groups by allowing users to allow/block lists of URLs.

E. Active mediation

The *ProKids* address bar icons as an age-differentiated feature are shown in Figure 3.4. On the left is an address bar message indicating that the user is visiting content with an appropriate age rating, while on the right is an address bar message indicating that the user is visiting inappropriate content, i.e. content with a higher age rating. They help children visit websites to either report abuse or learn about safe browsing.

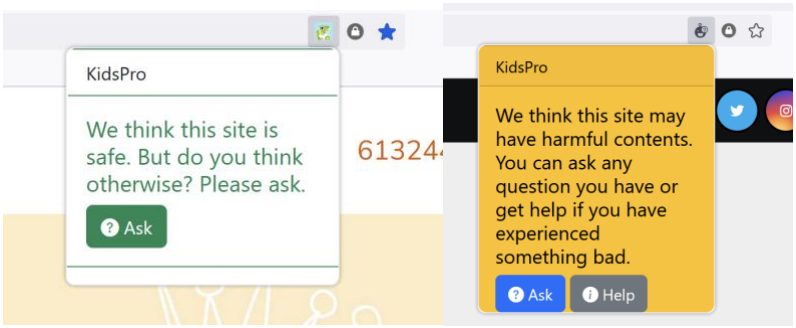


Figure 3.4 Help links and address bar feature of ProKids

F. Teen self-monitoring

The tool blocks the inappropriate content by default. Children over age 10 are treated differently and the contents are served but with a warning symbol and a notification pop-up as shown in as shown in Figure 3.4 and Figure 3.5. This feature is intended to make the child think about the content the child is accessing and hopefully make better decisions over time.

G. Teen impulse control

When older children try to access inappropriate content, they see a warning popup. It should make them pause to make a choice. This warning popup is shown in Figure 3.5

Figure 3.5 Warning pop-up notification shown to older children

H. Teen risk-coping

The address bar icon has links including a website where they can get immediate help if they need it as shown in Figure 3.4.

Table 3.2 shows how the features of the system fit into the values extended from the TOSS evaluation.

Table 3.2 ProKids features vs values extended from TOSS

		User settings on device only	Use of X.509 certificates to verify site age rating	Monitor access to inappropriate content	Set time limit	Content control by age groups	Teen only features	Content control by list	Address bar icons	Links to educational/ help/ reporting websites	Notification popup warning
Values in Design	Privacy	x	x	x			x				
	Age Ratings		x			x	x		x	x	
TOSS Framework	Monitoring			x			x				
	Restriction		x		x	x	x	x			
	Active mediation					x	x		x	x	x
	Teen self monitoring			x	x		x		x		x
	Teen impulse-control				x		x		x		x
	Teen risk-coping		x				x		x	x	x

3.1.3 Architecture

3.1.3.1 Age Ratings

ProKids enables content control by age group. The age groups are designed according to children's developmental stages [108]. For simplicity in implementation, a single or double-letter code represented each group.

a. P for 0-5 years old: preschool, preliterate and early literacy

b. E for 6-9 years old: core primary school years

c. T for 10-12 years old: transition years

d. ET for 13-15 years old: early teen, early years

e. MT for 16-17 years old: mid-teens, approaching adulthood

3.1.3.2 System Interactions

As for components in the system, governance, web server and web browser are involved as shown in Figure 3.6.

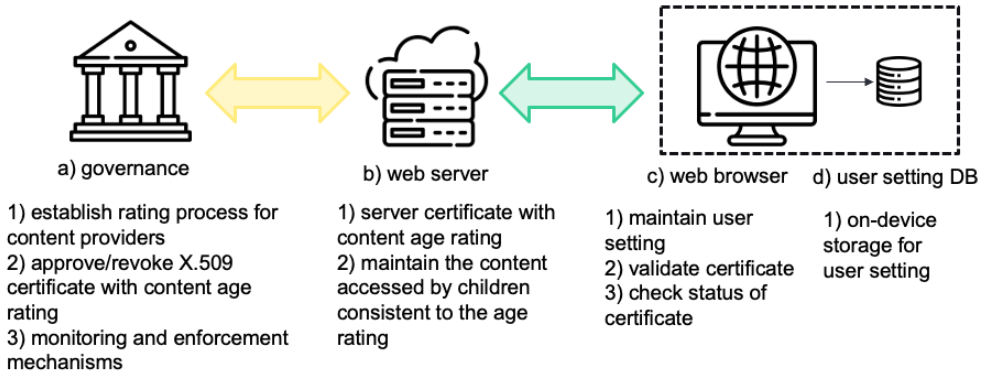


Figure 3.6 ProKids System Architecture

- Governance:

  Although the system requires some kind of governance to be in place, its implementation is out of scope in this study. The governance should include all agencies with a stake in regulating the Internet.

  ProKids provides links to two Canadian agency websites related to safe browsing and reporting inappropriate content from the browser plugin address bar icons.

  A governance body should assign age ratings to websites and they should be regularly checked to ensure compliance.

- Web server with content age rating:

  Content providers with websites that children access have their sites evaluated with proper age ratings by the appropriate governance bodies. The age ratings would then be included in their Certificate Signing Request (CSR) to create X.509 certificates. X.509 certificates would be created when approved with the age ratings by CAs who communicate with the governance bodies to match the age ratings.

- Web browser as a mediation tool:

  The browser has three main functionalities in *ProKids:* maintaining user settings, validating web server certificates and producing a monitoring report.

  1) Maintain user settings.
     a. User Interface
     b. Backend DB
  2) Validate web server certificate against age ratings.
     c. Validate against rule settings (e.g. the black/white list and time settings)
     d. Validate against user ratings

3) Monitor browser activities and store a monitoring report.

The browser fetches the user setting with the age rating on the device a child accesses and validates the age rating of the X.509 certificate against the user setting to decide whether to load or block the content.

The sequence of the browsing experience is shown in Figure 3.7.

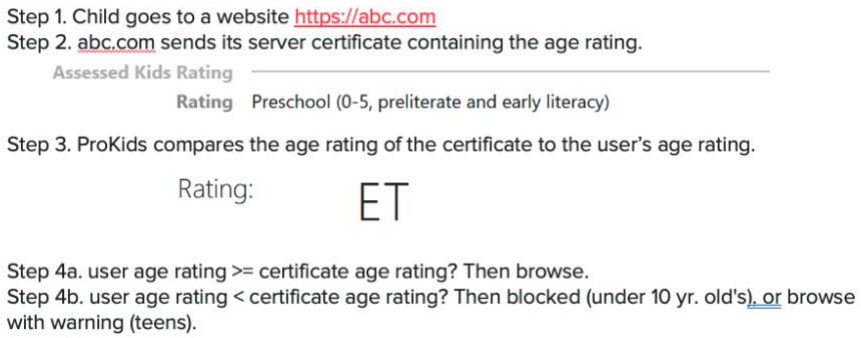


Figure 3.7 ProKids interaction sequence

3.2 System Implementation

This section contains implementation details of the proposed system.

3.2.1 X.509 Certificate with OpenSSL

A custom extension field was added to X.509 certificates for the system using OpenSSL commands.

The steps to create an X.509 certificate with the extension are as below. We used a self-signed CA to sign the certificates for convenience.

1) Create a configuration file for CSR

A new field *kidsAssProp* with an OID 1.3.6.1.4.1.60933 was added to a configuration file for a CSR as shown in Figure 3.8. The decimal 60933 was assigned by the Assigned Numbers Authority (IANA) to be unique.

```
[ new_oids ]
kidsAssProp = 1.3.6.1.4.1.60933.1

[ req ]
default_bits       = 2048
distinguished_name = req_distinguished_name
req_extensions     = v3_ext

[ req_distinguished_name ]
countryName                 = CA
stateOrProvinceName         = ON
localityName                = Locality Name (eg, city)
organizationName            = TEENLEARNING
commonName                  = TEENLEARNING
CN = teenlearning.ca

[ seq_sect ]

[ v3_ext ]
subjectAltName = @alt_names
keyUsage=nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage=serverAuth
kidsAssProp = ASN1:UTF8String:T
```

Figure 3.8 CSR configuration with a custom field

2) Create a private key

   openssl genrsa -out xxxx.key 4096

3) Create a CSR

   openssl req -config xxxx.cnf -new -key xxxx.key -out xxxx.csr

4) Sign the certificate

   openssl x509 -req -in xxxx.csr -CA cacert.pem -Cakey mycaKey.pem -out xxxx.crt -CAcreateserial -CAserial serial -days 365 -sha512 copy_extensions copyall

3.2.2 Browser add-on

The tool was developed as a Firefox browser add-on package using JavaScript, HTML5 and WebExtension tools on Visual Studio Code editor. A Firefox browser add-on was chosen for convenience as the development SDK had certificate validation details available. It was built as a desktop browser add-on but it is possible to develop a Firefox add-on for Android mobiles.

A. User settings

1) User interface

The user interface for settings included age rating, rule settings and display of monitoring report. The user settings are shown in Figure 3.9.

2) Data storage

The data for browser add-ons is stored locally on the operating system [109].

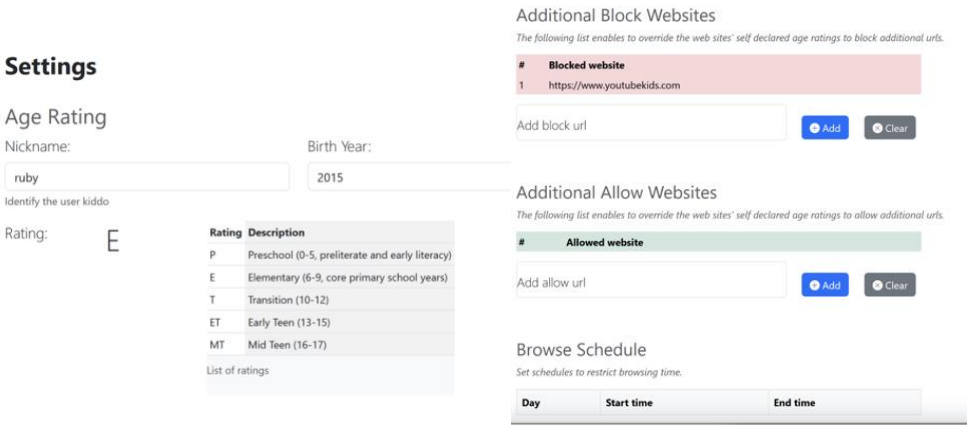


Figure 3.9 ProKids user settings

3) Password

For access control, the settings page was password enabled. The password was encrypted.

B. Certificate validation

A function to check the age rating of the certificate before content loading was written as in Figure 3.10 and Figure 3.11. This method extracts the age rating value from the certificate extension field and compares the user age rating fetched locally to determine the browser action. It works as a supplementary application authorization step using extension fields after a TLS handshake [110].

```
browser.webRequest.onHeadersReceived.addListener(
  details => {
    validateSite(details);
  },
  { urls: ["<all_urls>"], types: ["main_frame"] },
  ["blocking"]
);
```

Figure 3.10 Event listener to check site certificate

```
Function validateSite() {
   … check allowed time

   siteAccess = 'A';
   if (siteRating) {
      RatingMatched = siteRating <= userAgeRating
      If (!matched) {
         If (userAgeRating == p or e ) {
            siteAccess = 'B' //blocked for under 10
         } else {
            siteAccess = 'AW'; //allow with warning.
         }
      }

   }
   If (site belongs to allowedUrl) {
      siteAccess = 'A'; //allowed
   }
   If (site == blockedUrl) {
      siteAccess = 'BB'; // blocked
   }
   . . .

}
```

Figure 3.11 Pseudocode to validate age rating

C. Visual features for children

Several design considerations were put in place for children. The visual features, which include a notification pop-up, address bar symbols and links were implemented for scenarios shown in Table 3.3. The notification popup shown in Figure 3.5, grey address bar symbol and a help link are differentiated features for children older than 10 years old when they visit inappropriate sites as shown in Figure 3.4.

Table 3.3 ProKids visual features

Scenarios	Blocked?	Address bar symbol	Links	Alert notification
Visit a site with appropriate age rating		regular colourful symbol	A link for education /reporting	
Site is blocked or outside scheduled hour	Yes			
Child is < 10 years old and site has inappropriate age rating	Yes		A link for education /reporting	
Child is > 10 years old and site has inappropriate age rating		grey warning symbol	Links for education /reporting and help	Windows notification popup.

Chapter 4

Results

This chapter examines the test methods and detailed evaluations of the proposed system, including a comparison analysis and the initial exploratory user study that was employed. We discuss the results, limitations and future improvements at the end of the chapter.

4.1 Test

4.1.1 Test Configuration

For the initial tests, five web servers with content serving each age category were installed via a web hosting company (HostPapa) and X.509 server certificates with the custom extension field for age rating were installed.

Table 4.1 Web servers hosted for testing

Age rating	Age group (years)	Domain name	Site purpose
P	0-5	prokids.ca	Day care website
E	6-9	kidstreaming.ca	Video streaming for young children
T	10-12	teenlearning.ca	Educational site
ET	13-15	earlyteengames.ca	Game site for tweens and teens.
MT	16-17	midteenblogger.ca	Blogger site for midteens and up.

A. Website Hosts

A separate domain name represented each age group as shown in Table 4.1. A home page of the host with age rating E is shown in Figure 4.1. For example, the first domain 'prokids.ca' was created with an age rating 'P', and the second, 'kidsstreaming.ca', was created with an age rating 'E'.

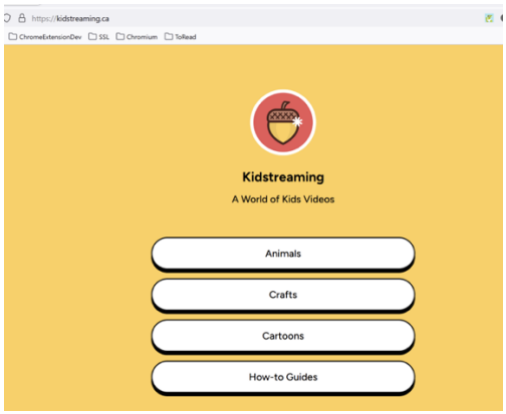


Figure 4.1 Home page of kidsstreaming.ca with age rating E

B. Certificate Viewer

A browser certificate viewer was implemented to map the custom field of the certificate to the age rating. It verified the certificate passed from the websites set up above. Figure 4.2 shows the certificate content of a host for *midteenblogger.ca*. The codes were updated from the original Firefox certificate viewer add-on [111].

Figure 4.2 Certificate extensions including age rating in certificate viewer

C. Browser

The Firefox plugin was installed and the websites above were successfully tested against various rule settings.

4.2 Initial Exploratory User study

This section contains details of the empirical investigation used in this study.

4.2.1 Design

An initial exploratory user study was conducted to validate the usefulness of the proposed system. The study consisted of a pre-survey, a demo of the system and a semi-structured interview followed by an exit survey. It was approved by the Office of Research Ethics and Integrity of the University of Ottawa in 2023[5]. The research questions that the initial exploratory user study was attempting to answer were:

[5] See 0 for approval

1) How does *ProKids* compare to traditional parental mediation applications?
2) What values do parents care about when choosing parental mediation tools?
3) What specific features in *ProKids* do parents find useful and not useful?

The combination of survey questions and interview questions also revealed the online activity styles of their children, their parental mediation styles and preferences with respect to parental mediation tools.

A. Pre-Survey Question Design

Please see Appendix H for a list of pre-survey questions asked. The pre-survey included sets of questions on demographics, children's online activities, parenting mediation styles and online risk experience. Some of the questions were pre-validated in another study [112] for measurements of family communication [113], parenting styles [114] as shown in Table 4.2, and online risk experience [115].

Table 4.2 Pre-survey questionnaire items of the parenting style scale

Factor	Survey Questionnaire Item
Involvement (i.e. responsiveness)	EC1. My child can count on me to help him/her out, if he/she has some kind of problem.
	EC3. I push my child to do his/her best in whatever he/she does.
	EC5. I keep pushing my child to think independently.
	EC7. I help my child with his/her schoolwork.
	EC9. When I want my child to do something, I explain why.

Factor	Survey Questionnaire Item
	EC11. When my child gets a poor grade in school, I encourage him/her to try harder.
	EC13. I know who my child's friends are.
	EC15. I spend time just talking with my child.
	EC17. My family does things for fun together.
Autonomy granting	EC2. I tell my child that you shouldn't argue with adults.
	EC4. I tell my child that he/she should give in on arguments rather than make people angry.
	EC6. When my child gets a poor grade in school, I make his/her life miserable.
	EC8. I tell my child that my ideas are correct and that he/she should not question them.
	EC12. I let my child make his/her own plans for things he/she wants to do.
	EC14. I act cold and unfriendly if my child does something I don't like.
	EC16. When my child gets a poor grade in school, I make him/her feel guilty.
	EC18. I won't let my child do things with me when he/she does something I don't like.
Strictness/supervision (i.e. demandingness)	EC21. How much do you try to know where your child goes at night?
	EC22. How much do you try to know what your child does with his/her free time?
	EC23. How much do you try to know where your child is most afternoons after school?
	EC24. How much do you really know where your child goes at night?

Factor	Survey Questionnaire Item
	EC25. How much do you really know what your child does with his/her free time?
	EC26. How much do you really know where your child is most afternoons after school?

B. Interview Questions Design

Please see Appendix G for a list of interview questions posed.

1) *ProKid*s as a parental mediation tool

Interview questions 'Q8 – Overall impression of the *ProKids* tool' and 'Q9 – Which features did you like? Why?' directly asked about impressions and liked/disliked features of *ProKids*. Responses to other questions such as Q3 also revealed the participants' opinions on *ProKids*.

2) Values parents care about in digital parenting mediation

Interview question Q7 dealt with what values the participants care about when selecting parental control/monitoring tools in terms of children's safety. Questions Q2, Q3 and Q6 were about features the participants like in parental control/monitoring tools in general.

3) On privacy and age-related controls

Interview question Q5 sought parents' thoughts on privacy when using parental control/monitoring tools.

C. *Data Gathering*

Recruitment was done via LinkedIn posts and 12 friends and professional contacts of the main researcher, who were selected on a first-come, first-served basis, participated in the initial exploratory user study. The screening criteria were for the participants to be over 18 years old and to have one or more children under 18 years of age. A $10 gift card was given to every participant after the initial exploratory user study.

The initial exploratory user study sessions were conducted between October and November 2023. During a confidential online survey, the respondents were asked about their children's online activities, their online parenting strategies and demographic questions with an average time of 8.45 minutes to complete. The participants were then asked to watch a demonstration of the *ProKids* features and of existing parental control tools if needed online via Zoom. During a follow-up interview, participants were asked questions about their perception of the system compared to other parenting mediation tools. The interview sessions were recorded and completed with an average of 30 minutes. The exit survey had a System Technical Acceptance Questionnaire that was pre-validated in studies by Ghosh et al. [111] and Davis [115]. It was completed within an average time of 1.02 minutes. The surveys were conducted on the Microsoft Form platform anonymously.

D. *Data Analysis*

The recorded interview sessions were stored in a password-protected computer. Their answers were cleaned, organized and categorized to answer the research questions. The responses were theme-coded by replaying and taking notes of the recorded sessions

iteratively. The initial 61 codes were coded into three codes in four coding steps. The codes were categorized for the following [117], [118]:

1) Features parents like in the parental control/monitoring tools
2) What values parents are most concerned about in terms of children's safety online
3) Mediation decisions

The survey results were downloaded and stored on a password-protected computer as well. The result was statistically analyzed using quantitative analysis.

4.2.2 Results

This section presents the findings from the initial exploratory user study sessions.

A. Participants

The pre-survey had demographic questions. 12 parents with children aged 5 to 17 years old, participated in the initial exploratory user study. Three participants were male and nine were female. Among them, there were 22 children under the age of 18 years old. The mean age of the children was 10.63 years old; the median age was 10.5 years old, and the mode age was 10 years old (see Figure 4.3). The demographics of survey respondents are shown in Table 4.3.

The participants' children generally engaged in various online activities, the highest portion of the children watched videos, used social media, sent and received text messages, played online games and browsed the Internet on a daily basis, once they started using it as shown in Figure 4.4. Participants had used and were using various parenting mediation tools, mostly free tools that come with devices or services they purchase as shown in Figure 4.5. Only one participant had not used any tool.

One participant out of the 12 answered “yes” to the online risk experience questions about whether their child was victimized online in both categories in online harassment and information breach.

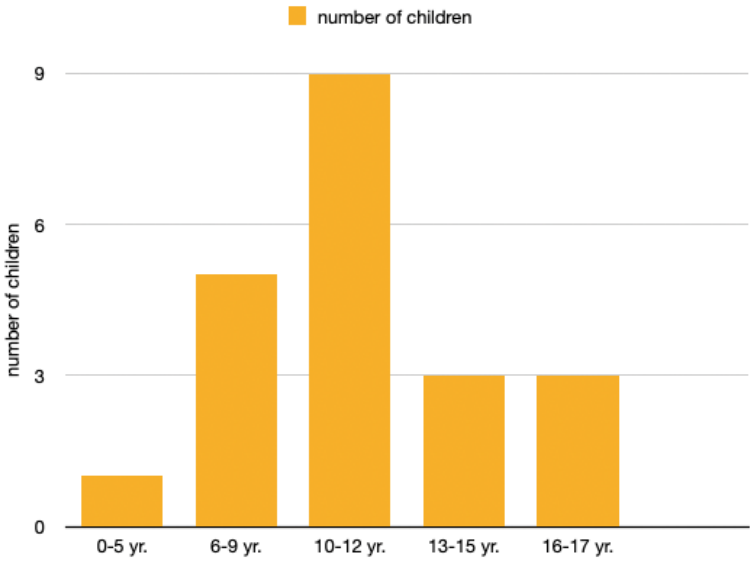


Figure 4.3 Number of children per age group

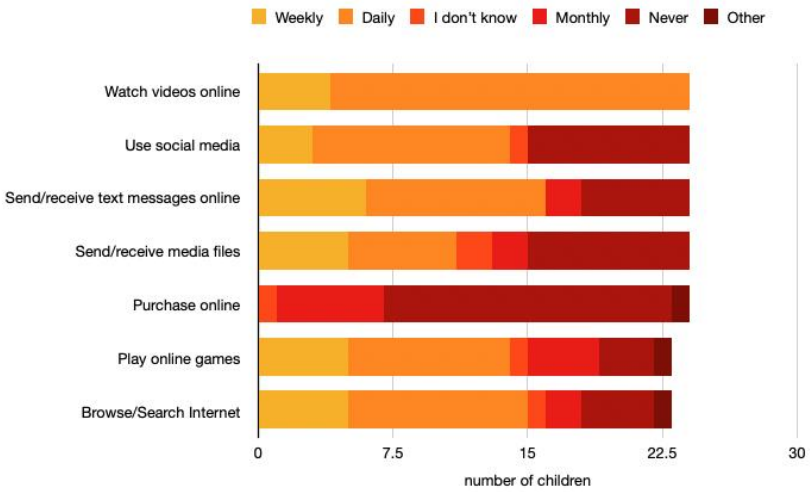


Figure 4.4 Children's online activities frequencies from the pre-survey

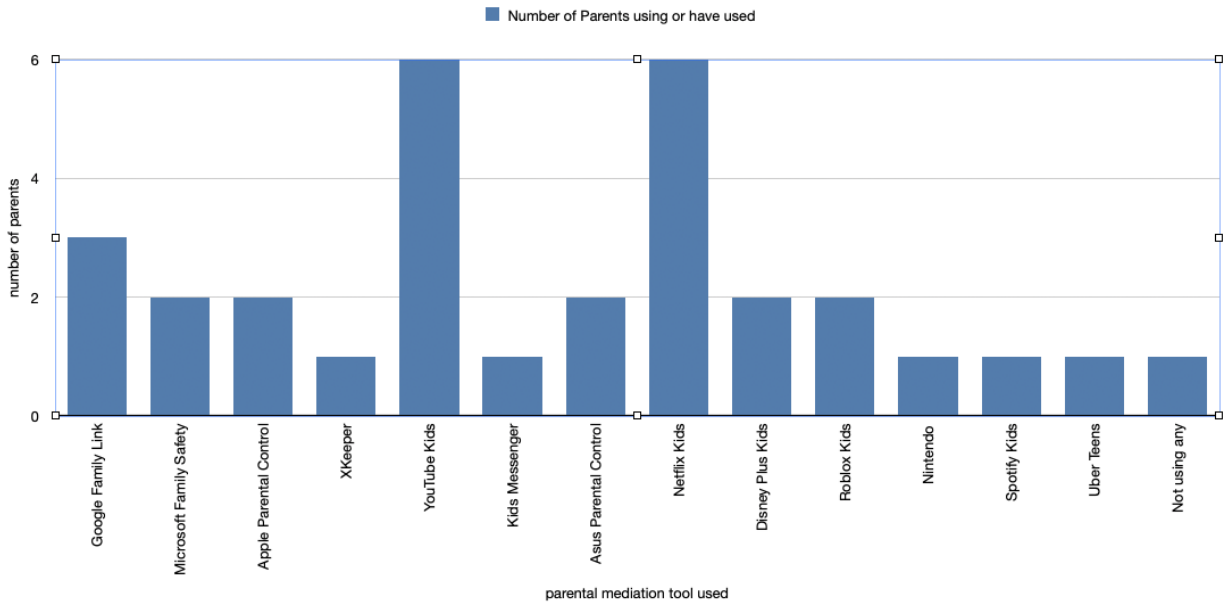


Figure 4.5 Parenting mediation tools used by parents

Table 4.3 Table 4.2shows the parenting styles of the respondents analyzed by the questionnaires for parenting style and communication styles. Each question item of involvement, autonomy granting and supervision index as shown in Table 4.2 was measured on a 5-point Likert scale. The self-reported parenting styles were analyzed by performing a mean split (i.e., high/low) on each index [112]. According to Ghosh [112], four parenting styles are assessed based on parents' involvement and demandingness: authoritative (high involvement, high demandingness), authoritarian (low involvement, high demandingness), permissive (high involvement, low demandingness) and neglectful (low involvement, low demandingness). Our data sets showed two parenting styles: authoritative (9) and permissive (3). Authoritative parents are associated with being *highly* responsive and *highly* autonomy-demanding. The authoritative parenting style is

the most optimal for children's development and their future as adults at the emotional, social and cognitive levels [119].

Table 4.3 Demographics of the respondents

	Gender	Age	Ethnicity	Children's ages	Education	Communication Index	Involvement Index	Autonomy demandingness Index	Supervision (Strictness) Index	Parenting Style
P1	Male	45-54	White/ Caucasian	9, 16	completed college degree	4	High	Med	4.33	Authoritative
P2	Female	35-44	Asian	13	bachelor's degree	3.75	High	Low	4	Permissive
P3	Female	35-44	Asian	7, 10	master's degree	5	High	Med	5	Authoritative
P4	Female	35-44	Asian	10, 11	bachelor's degree	3.25	High	High	4.5	Authoritative
P5	Female	35-44	Asian	11, 12	doctorate degree	4	High	High	5	Authoritative
P6	Female	45-55	Asian	13, 16	master's degree	3	High	High	4.7	Authoritative
P7	Male	45-54	Asian	6, 8	master's degree	3.5	High	Med	3.5	Authoritative
P8	Female	35-44	White/ Caucasian	4, 7, 10	master's degree	4.25	High	Low	5	Permissive
P9	Male	45-54	White/ Caucasian	8	bachelor's degree	3.75	High	Low	3.83	Permissive
P10	Female	55 years old or older	White/ Caucasian	12, 17	bachelor's degree	5	High	Med	5	Authoritative
P11	Female	45-54	Asian	10, 13	bachelor's degree	4.5	High	High	4.83	Authoritative

	Gender	Age	Ethnicity	Children's ages	Education	Communication Index	Involvement Index	Autonomy demandingness Index	Supervision (Strictness) Index	Parenting Style
P12	Female	45-54	Asian	11	doctorate degree	5	High	Med	4.67	Authoritative

B. ProKids Evaluation

1) First impression

Strong privacy and automatic content control by age groups and rating were mentioned by 10 out of 12 participants. They liked the fact that they did not have to share kids' information with the companies and the differentiated features for teens. Participant 5 (P5) said all kids use the Internet these days and the responsibility should not fall upon parents only. P3 said that contents are being restricted by default without having to know each of the sites, it feels safer and preventive as It is difficult to know everything in advance.

P11 liked that the system provided helpful links to other security platform websites. P10 said the system is great for privacy and age verification. Four participants mentioned that they liked they did not have to keep coming back to the settings to update the list of blocked/approved URLs as they are automatic, and It is preventive. The participants said that they would feel comfortable letting kids explore the web if the system was set up but 50% of the participants expressed concerns over whether the companies would be interested in implementing the rating in the certificates and governance would ever be there. Three participants said there should be some governance around the web and this kind of framework should have been there already.

2) Liked features

The following features were rated as favourites in *ProKids*. Age groups and warnings for teens were mentioned by most parents. And differentiated features for teens were appreciated by parents.

- Content rating by groups (7/12 participants)

  They liked that the content control could be automatically done without having to know the list in advance. Some participants said this would let kids explore and learn.

- Strong privacy (6/12 participants)

  These participants liked that no user setting information was shared with companies and that users instead had the option to make decisions while age was verified by authenticating the company using the certificates instead of the other way around. But P1 mentioned that It is weak privacy as the browser sometimes itself needs an account (i.e., Google account for Chrome browser) to open.

- Notification popup for warning (2/12 participants)

  Some parents with teens liked the fact that there were warning symbols and notification pop-ups to warn older children when they accessed blocked websites. They said this is good as children would find a way to get around if it was blocked, this would instead give them a chance to pause and think. P11 said ‘You are also giving the control to the child to make these important decisions and maybe they will choose right or maybe they will choose wrong, but at least they know It is a process they are going through making decisions of right and wrong. It is going to force them to think a little bit’. P11 thought that the warning should come in before the content loads so that they can choose to open the content or not.

- Monitoring

  Other participants liked getting monitoring reports of where the kids accessed while letting them explore more freely.

- Content control by list

  One liked the approved/blocked URL list as it makes the tool more flexible, rather than rigid.

3) Disliked features

- Realization of the system:

  Four participants expressed doubts that companies or governments would ever implement it.

- Mobile apps support:

  Many participants asked if *ProKids* could be implemented in mobile apps and P8 suggested working with companies like Apple and Microsoft AppStore to have the same ratings as their apps.

- Global standardization difficulties:

  Two participants mentioned potential difficulties in global implementation as age groups may be different in some countries. (The age groups can be implemented as variables in different countries in *ProKids*)

- More adjustable/flexible settings:

  Some parents wanted more flexible settings. For example, P3 preferred to stop propagation instead of showing warnings for teens. P4 wanted to receive email reports of the monitoring reports with different frequencies.

- Multiple sources in a website:

  Some participants questioned how multiple sources in some websites would be curated – images or links to other websites.

- Public computer:

  Some parents asked how *ProKids* would work in public computers.

C. Features Parents Like in Parental Control/Monitoring Applications

The functional features and usability features parents use and like most in parental control apps are listed here in the order of number of mentions. They confirm the common features we discussed in section 2.1.3.2.

1) Functional features

- Content control

  This includes blocking certain content of apps, filtering by content types, and limiting by age.

- Monitoring

  Many parental control tools and platforms (e.g., *Family Link and Netflix Kids* send monitoring reports to parents on a fixed or flexible frequency basis. Three parents said that they wanted to get the monitoring reports or alerts in real time so that they could stop or restrict their children immediately. Two of them already have these features. P9 said that he only uses the monitoring feature in Microsoft Family, and he has not explored other features saying he has left the features as a default.

- Screen time

  Three participants used the screen time feature in their applications.

2) Usability features

- Easy/simple setup and install

  Parents prefer simple setup and configuration features in their busy lives in order to save time. Some parents mentioned they have yet to set up their parental control/monitoring tools properly although they have already been using them with default settings.

- Granular/flexible settings

  Parents like granular setting options available to them such as age settings, on/off for each feature and adjustable reporting frequencies. They like to have flexible settings so that content control is not so rigid.

- Good default

  They liked to see good default settings in the apps they use in order to have a good base to start from. P9 said he would use *ProKids* as a default base and combine other applications with additional mediation features such as filtering.

D. Parental Values for Children Online

- *Content*

  Most parents were most concerned about adult or violent content and interaction with strangers on the web. Some parents mentioned dark patterns on the web such as showing ads and links to direct them to other websites unknowingly as concerns.

- *Interaction with others*

  Participants were concerned about their children interacting with strangers. They wanted to know who their children were interacting with on the game platforms

or social media. P11 said that age 13, which is the age allowed to create a social media account, is too low and it should be higher.

- *Privacy*

  A couple of parents mentioned privacy concerns with respect to social media.

- *Transition age*

  Four parents expressed concerns about content for their children in the transition age group. They said there is little in the way of proper content for them in age-rated apps such as *YouTube Kids* or *Netflix Kids* and that their children therefore go directly to adult content instead. Two parents mentioned that prevention is difficult for children at this age and it falls on parents' continuous efforts.

- *Consistent rating*

  Seven participants mentioned the importance of consistent ratings. P10 said that *Spotify Kids* sometimes play music with lyrics containing adult content. Several participants mentioned that *YouTube Kids'* content was not consistently rated. They indicated that its ratings were either too loose or too strict, and improper for the transition age group.

- *Education and communication*

  Four parents mentioned the importance of education and communication. They mentioned that It is important to educate children and above all to keep the communication lines open.

- *Trust*

  Two parents mentioned trust is most important with respect to mediating their children's online experience and that they trust their kids to make the right

decisions. Among them, P7 said she does not like to be monitored or controlled and feels the same when it comes to the kids.

E. Parental Mediation Decisions

The mediation styles analyzed from the interviews were generally the following. Parents in the study used a restrictive mediation strategy when the children were young and the children did not have opportunities to explore and learn how to browse safely when parents did not use active mediation strategy such as their communication and education. Parents who did not have proper technical mediation tools when the children were young, were left helpless when the kids were in the transition age group as the children tried to explore themselves and got into trouble.

1) Kids are young and we are in control (restrictive & monitoring)

   Six participants who had young children (younger than 12 years old) were confident that the kids only accessed the sites or apps the parents approved of as they were always around when their children were online. The children only had access to online devices around the parents only.

2) Communication and education (active mediation)

   Four parents mentioned that they try to talk about safe browsing tips such as how not to open emails or links they do not know of.

3) Neglect (passive)

   a. With a feeling of helplessness in terms of external support

   Five parents expressed feelings of helplessness in terms of parental control/monitoring for children. They either had not gotten chances to find the right tools or had not set them up properly though they felt they would like to if they were

not constrained by either a lack of time or knowledge. Two of them said they wanted to give kids freedom but this was difficult as they did not know how to. P10 said her child has accessed adult content through a Pokémon card ad shown on a website he visited.

Four of these parents expressed a willingness to explore and set up new features of the parental control apps despite the limitations they have. P11 said that she would like to get more insights but has not applied any specific restrictions.

b. No control when kids get older

Some parents had no control intentionally as kids were getting older. Three parents of children in the transitional age group or teens said their kids are already rejecting the controls they are subject to and P12 said It is too late to do anything for kids.

P2 said It is impossible to have restricting content for older kids and she is only using monitoring features.

F. ProKids System Technical Acceptance

The exit survey analysis showed that all parents accepted *ProKids* positively and believed that the system would be useful in keeping their children safe online (Q6) as shown in Table 4.4 [116]. All questions that measured the usefulness of the system were answered with high numbers (> 4 on a scale of 1-5).

Table 4.4 Descriptive statistics for technology acceptance model questionnaire response for ProKids (with 1-5 Likert scale)

Usefulness variable to keep children safe online	Mean	Median	Standard Deviation
Work more quickly	4.25	4.5	0.87
Job performance	4.17	4	0.83
Increase productivity	4.42	4	0.51
Effectiveness	4.25	4	0.75
Makes job easier	4.17	4	0.72
Usefulness	4.42	4	0.51

4.2.3 Limitations of the Initial Exploratory User Study

More participants would have been beneficial in analyzing parenting mediation styles and perceptions of the proposed system. A reliability Kappa value could not be calculated due to the small sample size. Using the lens of VSD, we only conducted the user study on parents, not on other stakeholders such as governance practitioners, content providers or children.

4.3 System Comparison and Limitation

This section compares the features among the existing parental control/monitoring tools and the proposed system *ProKids.* The complete comparison analysis is shown in Table 4.5.

Table 4.5 ProKids values vs other parental mediation tools

		ProKids	Circle of Trust [104]	Teen-Alyze [45]	FamiLync [26]	Apple Parental Control [120], [121]	Google Family Link [122], [123]	Microsoft Family Safety [124]	YouTube Kids [125], [126]	Netflix Kids [127], [128]	Roblox [129], [130]
Privacy - degree of identifiability, network centricity	Children's identity - anonymous (unlinkable)	x									
	Children's identity - pseudonymous (not linkable with reasonable effort)	x							x	x	
	Data in user sphere (client centric)	x									
	Only record the dangerous access	x	x								
	Age verification anonymously	x									
Age Group (rating)	Rated content by age group	5 age groups							3 group under 12	maturity ratings	2 groups under 18
	Children's age range	0~17	13~17	13~17	13~17	0~17	0~17	0~12	0~12	0~12	0~12
Parental Monitoring	Monitor access to content or usage	x	x	x	x	x	x	x	x	x	x

		ProKids	Circle of Trust [104]	Teen-Alyze [45]	FamiLync [26]	Apple Parental Control [120], [121]	Google Family Link [122], [123]	Microsoft Family Safety [124]	YouTube Kids [125], [126]	Netflix Kids [127], [128]	Roblox [129], [130]
Parental Restriction	Set time limit	x		x	x	x	x	x		x	x
	Content control by age group (default)	x							x	x	x
	Content control by filter					x		x	x		
	Content control by list	x				x	x	x	x	x	
	Chat filter										x
Active Mediation	Adjustable age group	x								x	x
	Teen only features	x	x	x	x						
	Educational/reporting/help links	x							x		x
	Inappropriate contents warning/notifications	x									
	Risk flags/sentiment analysis, word cloud		x								
	Request/grant more time			x							
Teen Self-monitoring	Inappropriate contents warning/notifications	x									
	View teens' app usage		x	x	x						
	View exceeding allotted time	x		x	x						

		ProKids	Circle of Trust [104]	Teen-Alyze [45]	FamiLync [26]	Apple Parental Control [120], [121]	Google Family Link [122], [123]	Microsoft Family Safety [124]	YouTube Kids [125], [126]	Netflix Kids [127], [128]	Roblox [129], [130]
	Risk flags/sentiment analysis		x								
Teen Impulse-control	Inappropriate contents warning/notifications	x									
	Risk flags/sentiment analysis, word cloud		x								
	View exceeding allotted time	x		x	x						
Teen Risk-coping	Help link	x									
	Inappropriate contents warning/notifications	x									
	Risk flags/sentiment analysis, word cloud		x								

ProKids is built with features that try to balance all parental mediation strategies such as monitoring, restriction and active mediation in addition to enhanced privacy. The combined strategies allow children to gain development opportunities while reducing potential risks online. Most commercial parental control/monitoring tools have functional features that meet parental restriction and parental monitoring, but lack active mediation, strategies for teens and privacy controls.

A. Privacy

ProKids protects children's privacy through anonymity and unlinkability. Data is stored in the user sphere resulting in a less network-centric architecture. *ProKids* collects the minimal data needed just 'birth year' instead of 'birthdate' while many other tools require an entire parental profile and children's profile including email addresses, contact information and birthdates. As for unlinkability, some tools use pseudonyms in profiles (e.g., *Netflix Kids*) but reidentification can happen as the parental account is linked to the profiles. All other tools offering monitoring features store children's online activity history online which raises privacy risks in the long-term.

ProKids and *Circle of Trust* provided children with some privacy by not giving the entire access history, but only the access history of flagged contents to the parents.

B. Age Ratings

Video content on *YouTube Kids* and *Netflix Kids*, and game content on *Roblox* have ratings but only up to age 12. Most of the commercial applications also have content ratings up to age 12. The parental mediation tools in the compared studies [26], [45], [104] were specifically designed for teens only. The mediation features in *ProKids* apply to kids aged 0-17. While most restrictions are only applicable for children up to 12 in commercial tools, children can choose to stop parental supervision when they turn 13 years old in *Apple Parental Control* and *Google Family Link*.

C. Parental Monitoring

All tools considered had some mechanism for parental monitoring functionality.

D. Parental Restriction

While *ProKids* has automatic content control by aged-rated content, some tools have content filters or chat filters. Most tools with traditional techniques badly filter user-generated content [27]. In the *ProKids* system, we envision that these filter mechanisms should be applied before the ratings process so they will not be needed ideally, or they can be used as extra measures for cautious parents.

E. Active Mediation

Granular and adjustable content controls enable active mediation, some tools such as *Google Family Link* or *Apple Parental Control* require a setup of new profiles/settings to change the age group or ratings. Showing teens what stage they are at in terms of using allowed time or accessing adult content enables active mediation. *Teen-Alyse* has a feature of teens asking for more time and parents granting time to promote parent-teen communication.

F. Teen self-monitoring

The studies had features for teen self-monitoring such as viewing their own usage and noticing the flagged contents.

G. Teen impulse-control

These features as above also enable teens to understand their situations and regulate their impulsive behaviour.

H. Teen risk-coping

Circle of Trust achieves teen risk-coping by showing teens risk flags, sentiment analysis and, a word cloud. Similarly, *ProKids* displays warnings and notification popups for

inappropriate content but also provides a help site where teens can seek coping assistance.

4.4 Discussion and Future Improvement

The initial exploratory user study and system comparison revealed some room for improvement in the current version of *ProKids*. We explain this in relation to the values considered as future improvement items.

A. Privacy

- User settings data

  Although the user interface was locked down with an encrypted password for the user settings, the data itself is on the system level and anyone with administrator access can access it. A more secure database with access control would improve privacy.

- Support for multiple browsers

  The proposed system implemented the client mediation tool as a Firefox add-on for convenience. To handle multiple browsers, each browser must implement the rating validation as part of browser certificate validation.

B. Age Ratings

- Use of the X.509 certificate

  The proposed system utilized a custom extension field of the certificate structure. For children to browse more freely on the Web, more websites with matching age ratings should be available for the system.

- Content age ratings vs. age verification

  The proposed system enables verifying the age rating of the contents as part of the authentication of web servers using the PKI system. This will ensure children freely explore age-appropriate content while preventing them from accessing inappropriate websites. If all websites implemented the age rating in their certificates, this might unburden the responsibilities of age-verification mechanisms on the websites. But what if the children access websites from public devices or crack the user settings so that they can access adult websites? This kind of problem exists in all current mediation tools as children these days are digitally skilled. Age-verification might still be required on websites with adult content to mitigate this.

C. Parental Monitoring

- Email monitoring report

  Participants in the user study wished to receive the monitoring report in emails with adjustable frequencies. Also, some parents wished to get an immediate notification in an email for prompt intervention in case children are in danger. As to email address is personally identifiable information, how It is stored and access to it should be carefully considered in any app making use of email addresses.

D. Parental restriction

- Adjustable options

  The existing features could be more flexible. For example, some parents wished that barring teens from inappropriate content was an option so that they could decide whether

their children access such content or not. Options could also be implemented for the email frequencies or email monitoring report mentioned above.

E. Active mediation & teen self-monitoring

The *Teen-Alyse* by Sangal et al. [45] has the functionality allowing for teens to ask parents to grant them more time and allowing teens to view monitoring reports themselves. This can promote active mediation and teen self-monitoring.

F. Teen impulse control

- Warning notification popup before the content loading

ProKids allows teens to access inappropriate content but displays a warning address bar symbol and a popup notification. Some parents wanted the content loading to come after children respond to the warning notification so that they do not have to see the content at all if they choose not to.

G. Teen risk-coping

- Links to education/reporting/help websites

The links implemented in *ProKids* are Canadian websites set up by Canadian government agencies or non-profit organizations. They could be varied for different countries.

H. VSD

- A more iterative approach of designing the system alternating conceptual, empirical and technical investigations is recommended.

I. Other

- Mobile application support

The tool can be implemented for mobile browsers. The governing body should ensure that mobile applications with relevant websites should have the consistent age ratings across the platforms.

- Multiple users or public computer

  We assumed a single user setting per desktop computer profile which should also apply to most devices. This should work for shared devices at home, but it would be difficult to set up profiles on public computers as mentioned above in B. It may be possible to auto-configure *ProKids* using login profiles from public computers that have set user profiles (e.g. a city library) to create the *ProKids* profile.

- Children trying to access content intended for older people

  ProKids has an administrative password feature to prevent children from accessing and changing their user profiles. But there is no prevention for children who acquire the password or for children who otherwise get around the measures to access harmful content. For instance, a younger child logging into his/her older sibling's device profile could not be prevented from accessing sites intended for the older sibling. Parents should be aware of this risk and take appropriate preventive measures.

Chapter 5

Conclusion and Future Directions

The primary goal of parental mediation is to prevent harm and promote online opportunities while maintaining trust and communication between parents and children. Parenting mediation tools are only one small part of the ecosystem for children's online safety and a single tool will not solve all the mediation difficulties or security risks that parents and children may encounter today [27]. This study looked at recommended parenting mediation strategies and trends with respect to technical mediation methods provided by industry and governments while identifying the main stakeholders in the nurturing ecosystem of children's development. Government and industry are responding to the needs of children online, but more proactive, rather than reactive, methods are required.

We identified gaps in current methods and proposed a system, *ProKids. ProKids* was designed using a Value Sensitive Design lens with values for *privacy* and *age ratings* in addition to TOSS strategies. Each of the values was carefully implemented while utilizing PKI to support *privacy* and age ratings. The system ensures enhanced privacy for children and automatic content control by *age ratings* with the help of the industry and government. The client tool, which has been built as a browser add-on, works as a parental mediation tool balancing parental mediation strategies and teen self-regulation strategies while equipped with the most common features of existing parental mediation tools. Features, usability and technical acceptance were measured and these proved the application's usefulness during the initial exploratory user study and the comparison analysis. Parents thought that the proposed system would be effective in providing automatic control of age-appropriate contents, in ensuring the privacy of data not leaving the device and in

providing differentiated features for younger, and older children. Children in the transition group required more special care in providing guidance and proper content.

Parental mediation styles are affected by children's digital skill sets and the risk awareness of the parents and children being considered. We hope that using a parental mediation tool such as *ProKids,* which can help educate children and parents about online safety, while enabling children to explore the Internet better, will positively influence parental mediation styles in the future. Parents should be aware that online security does not happen automatically and there are always risks. For example, children can get around the measures to access content older for them.

This thesis also identified existing gaps in the field of children's digital ecosystem and suggested the following areas for future study:

1) Age verification: Age verification is required on many websites as a result of new policies and regulations. Consistent and effective methods of verifying ages will be necessary with the highest degree of privacy provided for children.

2) Governance on age rating of Internet content: As mentioned in section 2.1.2.4, there are few studies on how to rate Internet content by age properly. As a result, commercially available parental mediation tools implement their own inconsistent ratings, confusing parents and children alike. Also, a consistent rating between mobile apps, content and games is desirable.

3) Transition age group (10-12 years old): The study revealed that there is hardly any support (i.e., no proper content or guidance) for children in this age group. More studies are needed to understand the requirements of, and to offer guidance for, this group.

4) Filling gaps between regulators, facilitators and the users: There are policies developed by regulators; there are also educational and help websites. But the children and parents who are to benefit from them are not aware of them. It is important to implement policies and regulations

and then communicate to all stakeholders who are affected so that they are aware of their rights and responsibilities.

Glossary

Catfishing: It is an “online dating” using a fake profile and false information in order to trick someone into believing that it is a real person.

Cheating in game: This means not playing by the rules of a game or plying in a way that is an outright violation of the way we expect games to be played using hacks and bots.

Children’s advertising: This is any dissemination of a product or service aimed at children, with the intention of selling to them. Cookies, data collection and child digital influencers on YouTube channels may all be used in children’s advertising, sometimes with negative consequences for children’s behaviour and their relationship with their parents.

Coding: This is a type of qualitative data analysis strategy. It is the activity of assigning labels to observations from text or other qualitative data forms.

Dark Patterns: These are tricks used in websites and apps that can make children do things they didn’t mean to , like buying or signing up for something. Dark patterns can negatively influence people’s behaviour and hinder their ability to keep their online privacy safe according to GDPR.

Dissing: This is a type of online denigration that consists in spreading cruel information about a victim through the Internet. Generally, the bully seeks to embarrass, shame, and ruin reputations and friendships. For children and adolescents, dissing, as well as other types of cyberbullying, can cause serious psychosocial, self-esteem and social problems.

Doxing: Doxing is a form of cyber harassment involving the public release of personal information that can be used to identify or locate an individual, such as home address, phone number or school information. This public release of an individual’s private, sensitive or personal information is an infringement of the right to privacy

Flaming: This is a hostile interaction between internet users through offensive messages that may cause emotional harm to victims.

Frapping: Frapping is "an activity that involves the unauthorized alteration of information on an individual's online social network site (SNS) profile by a third party. In most cases, the frappist posts inappropriate content in the victim's name constituting a kind of cyberbullying or trolling in order to ruin the target's reputation.

Griefing: Griefing attacks are a major problem whereby an adversary intentionally exhausts the channel capacity of the network. Griefing is also the name of a practice in online games whose purpose is to upset players. A griefer is a player who does not care about the progress of the game or the victory. This practice interferes with the fun of other users, whether with span in chat or offensive and/or abusive messages.

Happy slapping: Happy slapping is a form of cyber victimization that consists of recording a session while a person is being bullied in order to later circulate the recorded session to others.

Identifiability: This is the degree to which data can be directly attributed to an individual.

Internet Assigned Numbers Authority (IANA): The IANA is responsible for allocating and maintaining unique codes and numbering systems for Internet protocols.

k-anonymity: A concept that describes the level of difficulty associated with uniquely identifying an individual. The value k refers to the number of individuals to whom a pattern of data, referred to as quasi-identifiers, may be attributed. If a pattern is so unique so that k equals one person, the system is able to uniquely identify an individual.

Masquerading: This relates to any situation in which a bully may create a fake identity to harass someone. It may include the creation of a fake email address, instant messaging in other people's names or even the use of someone else's email or mobile phone. Masquerading can make it appear as if the threats have been sent by someone else, keeping the bully's identity hidden.

Natural Language Processing (NLP): This is a machine learning technology that gives computers the ability to interpret, manipulate, and comprehend human language.

Network centricity: This is the degree to which a user's system relies on a network infrastructure to provide a service as well as the degree of control a network operator can exercise over a clients' operations.

Object Identifier (OID): Object identifiers to name fields and sets of fields within an X.509 certificates. Each object identifier also indicates the representation for the selected field of fields.

Online challenges: Online challenges spread through SNSs. Usually there is an activity to be performed, recorded and shared on networks. The problem is that some challenges can be put the health of children and adolescents at risk. In Brazil, a student died during a challenge from hitting her head off the ground and suffering head trauma.

Online grooming: Tactics abusers deploy through the Internet to sexually exploit children. Grooming is a complex and lengthy process by which an adult builds an online relationship of trust and influence over a minor in order to obtain some type of sexual interaction, either online or offline.

Outing: A type of cyberbullying that consists of sharing someone's stuff with no permission.

Phishing: A fraudulent action characterized by attempts to acquire data from another person, usually through emails, websites and applications or SMS tokens. Fraudsters generally request registrations or update registration data through forms, posing as a person, institution or company.

Qualitative analysis: Qualitative analysis focuses on the nature of something and can be represented by themes, patterns, and stories.

Quantitative analysis: Quantitative analysis uses numerical methods to ascertain the magnitude, amount, or size of something.

Roasting: A type of cyberbullying which involves people asking to be insulted by posting photos or videos of themselves on SNSs usually with the hashtag #roastme. Roasting is dangerous for kids and teenagers due to the reactions this can provoke in them. Psychiatrists believe that there may be a prior psychological motivation for roasting, such as depression and/or anxiety and asking to be roasted may be a "self-destructive" behaviour.

Sharenting: The word combines the words "share" and "parenting". Sharenting is a practice of a family using SNSs to publish and communicate detailed information about their children. New concerns are raised like exposing children to pedophiles or online grooming, moreover data mining, marketing and facial recognition. The practice raises many responsibilities regarding privacy, image protection and digital self-representation.

Swating: Special Weapons and Tactics (SWAT) is a type of online prank with fraudulent 911 calls, generally applied on users of online gaming platforms.

Technological Pedagogical Content Knowledge (TPCK): Now known as TPACK, or technology, pedagogy and content knowledge. It represents a full understanding of how to teach with technology. The point of TPACK is to understand how to use technology to teach concepts in a way that enhances student learning experience.

Trolling: May be defined as a conversation or entire community posting incendiary statements or stupid questions onto a discussion. This phenomenon is present across internet cultures and can often be associated with sexualized aggression, threat and verbal abuse to silence women in cyberspace.

Visual hacker: It is the act of gathering information from another person or knowing what the other is doing online by visual means, such as through the reflection of the screen trying to figure out an administrator password or searching the keyboard for traces of the keys typed.

References

[1] "Safer Internet Day 2023, fighting to protect children online," World Economic Forum. Accessed: Dec. 27, 2023. [Online]. Available: https://www.weforum.org/agenda/2023/02/safer-internet-day-2023-bolstering-the-fight-to-protect-children-online/

[2] S. Ali, M. Elgharabawy, Q. Duchaussoy, M. Mannan, and A. Youssef, "Betrayed by the Guardian: Security and Privacy Risks of Parental Control Solutions," in *Annual Computer Security Applications Conference*, Austin USA: ACM, Dec. 2020, pp. 69–83. doi: 10.1145/3427228.3427287.

[3] R. M. M. Fernandes, L. F. R. da Costa Carmo, and C. L. R. da Motta, "A taxonomy proposal of cyber threats involving children and adolescents," in *2022 XVII Latin American Conference on Learning Technologies (LACLO)*, IEEE, 2022, pp. 01–08. Accessed: Dec. 27, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10013466/

[4] A. Prasad, R. Ruiz, and T. Stablein, "Understanding Parents' Concerns with Smart Device Usage in the Home," in *HCI for Cybersecurity, Privacy and Trust*, vol. 11594, A. Moallem, Ed., in Lecture Notes in Computer Science, vol. 11594. , Cham: Springer International Publishing, 2019, pp. 176–190. doi: 10.1007/978-3-030-22351-9_12.

[5] H. Hartikainen, N. Iivari, and M. Kinnula, "Should We Design for Control, Trust or Involvement?: A Discourses Survey about Children's Online Safety," in *Proceedings of the The 15th International Conference on Interaction Design and Children*, Manchester United Kingdom: ACM, Jun. 2016, pp. 367–378. doi: 10.1145/2930674.2930680.

[6] S. M. Gaiha, L. K. Lempert, and B. Halpern-Felsher, "Underage youth and young adult e-cigarette use and access before and during the coronavirus disease 2019 pandemic," *JAMA Netw. Open*, vol. 3, no. 12, pp. e2027572–e2027572, 2020.

[7] S. Ali and Elgharabawy, Mounir, "Suzan Ali, Mounir Elgharabawy, Quentin Duchaussoy, Mohammad Mannan, and Amr Youssef".

[8] A. Mathur, M. Kshirsagar, and J. Mayer, "What Makes a Dark Pattern... Dark?: Design Attributes, Normative Considerations, and Measurement Methods," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, Yokohama Japan: ACM, May 2021, pp. 1–18. doi: 10.1145/3411764.3445610.

[9] "BBFC-Young-people-and-pornography-Final-report-2401.pdf." Accessed: Dec. 27, 2023. [Online]. Available: https://www.revealingreality.co.uk/wp-content/uploads/2020/01/BBFC-Young-people-and-pornography-Final-report-2401.pdf

[10] A. Hiniker, H. Suh, S. Cao, and J. A. Kientz, "Screen Time Tantrums: How Families Manage Screen Media Experiences for Toddlers and Preschoolers," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, San Jose California USA: ACM, May 2016, pp. 648–660. doi: 10.1145/2858036.2858278.

[11] "Home," socialmedia.utah.gov. Accessed: Dec. 27, 2023. [Online]. Available: https://socialmedia.utah.gov/

[12] "Digital safety: Applying human rights in the digital world," World Economic Forum. Accessed: Dec. 27, 2023. [Online]. Available: https://www.weforum.org/impact/online-digital-safety/

[13] "How COPPA Came About | InformationWeek." Accessed: Dec. 27, 2023. [Online]. Available: https://www.informationweek.com/it-leadership/how-coppa-came-about

[14] "ICO slams Scottish Children's Reporter Administration for data breaches," Infosecurity Magazine. Accessed: Dec. 27, 2023. [Online]. Available: https://www.infosecurity-magazine.com/news/ico-slams-scottish-childrens-reporter/
[15] "Arizona State Agency Loses Data on 40,000 Children," CSO Online. Accessed: Dec. 27, 2023. [Online]. Available: https://www.csoonline.com/article/522586/arizona-state-agency-loses-data-on-40-000-children.html
[16] Z. Siddiqui and N. Zeeshan, "A survey on cybersecurity challenges and awareness for children of all ages," in *2020 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*, IEEE, 2020, pp. 131–136. Accessed: Dec. 27, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9231229/?casa_token=89YbkF52UxYAAAAA:C-_62n2lstMHeOWS-DAZaNblL59dam9kKUHyo8EiBa2sAtY4bT8C27Q2p7BJbITTbz43HXw3EDE
[17] S. Spiekermann and L. F. Cranor, "Engineering privacy," *IEEE Trans. Softw. Eng.*, vol. 35, no. 1, pp. 67–82, 2008.
[18] C. Kernaghan, "The Dark UX patterns targeting children," Medium. Accessed: Dec. 27, 2023. [Online]. Available: https://uxdesign.cc/the-dark-ux-patterns-targeting-children-6c6cb1f0624d
[19] Y. Zou, A. H. Mhaidli, A. McCall, and F. Schaub, "' I've Got Nothing to Lose': Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach," in *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 2018, pp. 197–216. Accessed: Dec. 27, 2023. [Online]. Available: https://www.usenix.org/conference/soups2018/presentation/zou
[20] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, and A. L. Toombs, "The Dark (Patterns) Side of UX Design," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, Montreal QC Canada: ACM, Apr. 2018, pp. 1–14. doi: 10.1145/3173574.3174108.
[21] G. Wang, J. Zhao, M. Van Kleek, and N. Shadbolt, "Informing Age-Appropriate AI: Examining Principles and Practices of AI for Children," in *CHI Conference on Human Factors in Computing Systems*, New Orleans LA USA: ACM, Apr. 2022, pp. 1–29. doi: 10.1145/3491102.3502057.
[22] "The digital world is a dark, dangerous place for children - here's how we can change that," World Economic Forum. Accessed: Dec. 27, 2023. [Online]. Available: https://www.weforum.org/agenda/2019/11/internet-safer-for-children-web-parents-digital/
[23] R. D. Kalinowski, Y. Xu, and K. Salen, "The Ecological Context of Preschool-Aged Children's Selection of Media Content," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, Yokohama Japan: ACM, May 2021, pp. 1–14. doi: 10.1145/3411764.3445429.
[24] P. C. Kumar, M. Chetty, T. L. Clegg, and J. Vitak, "Privacy and Security Considerations For Digital Technology Use in Elementary Schools," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, Glasgow Scotland Uk: ACM, May 2019, pp. 1–13. doi: 10.1145/3290605.3300537.
[25] M. Ko, S. Choi, S. Yang, J. Lee, and 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*, Osaka Japan: ACM, Sep. 2015, pp. 867–878. doi: 10.1145/2750858.2804283.

[26] "- SIP Benchmark III." Accessed: Dec. 27, 2023. [Online]. Available: https://sipbench.eu/transfer/FullStudyonparentalcontroltoolsfortheonlineprotection%20ofchildren.pdf
[27] E. B. Blancaflor, G. A. J. Anson, A. M. V. Encinas, K. C. T. Huplo, M. A. V. Marin, and S. L. G. Zamora, "A Vulnerability Assessment on the Parental Control Mobile Applications' Security: Status based on the OWASP Security Requirements," in *The 11th Annual International Conference on Industrial Engineering and Operations Management, Singapore*, 2021. Accessed: Dec. 27, 2023. [Online]. Available: http://ieomsociety.org/singapore2021/papers/1104.pdf
[28] S. Ali, M. Elgharabawy, Q. Duchaussoy, M. Mannan, and A. Youssef, "Parental controls: safer internet solutions or new pitfalls?," *IEEE Secur. Priv.*, vol. 19, no. 6, pp. 36–46, 2021.
[29] B. Burroughs, "YouTube Kids: The App Economy and Mobile Parenting," *Soc. Media Soc.*, vol. 3, no. 2, p. 205630511770718, Apr. 2017, doi: 10.1177/2056305117707189.
[30] T. Crepax, V. Muntés-Mulero, J. Martinez, and A. Ruiz, "Information technologies exposing children to privacy risks: Domains and children-specific technical controls," *Comput. Stand. Interfaces*, vol. 82, p. 103624, 2022.
[31] S. Livingstone, K. Ólafsson, E. J. Helsper, F. Lupiáñez-Villanueva, G. A. Veltri, and F. Folkvord, "Maximizing opportunities and minimizing risks for children online: The role of digital skills in emerging strategies of parental mediation," *J. Commun.*, vol. 67, no. 1, pp. 82–105, 2017.
[32] M. Nouwen, N. JafariNaimi, and B. Zaman, "Parental controls: reimagining technologies for parent-child interaction," in *Proceedings of 15th European Conference on Computer-Supported Cooperative Work-Exploratory Papers*, European Society for Socially Embedded Technologies (EUSSET), 2017, pp. 18–34. Accessed: Dec. 27, 2023. [Online]. Available: https://lirias.kuleuven.be/1860285?limo=0
[33] J. Yu, A. DeVore, and R. Roque, "Parental Mediation for Young Children's Use of Educational Media: A Case Study with Computational Toys and Kits," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, Yokohama Japan: ACM, May 2021, pp. 1–12. doi: 10.1145/3411764.3445427.
[34] K. Badillo-Urquiola, C. Chouhan, S. Chancellor, M. De Choudhary, and P. Wisniewski, "Beyond Parental Control: Designing Adolescent Online Safety Apps Using Value Sensitive Design," *J. Adolesc. Res.*, vol. 35, no. 1, pp. 147–175, Jan. 2020, doi: 10.1177/0743558419884692.
[35] B. Friedman, P. Kahn, and A. Borning, "Value sensitive design: Theory and methods," *Univ. Wash. Tech. Rep.*, vol. 2, no. 8, 2002, Accessed: Dec. 27, 2023. [Online]. Available: http://faculty.washington.edu/pkahn/articles/vsd-theory-methods-tr.pdf
[36] P. B. Friedman, H. Kahn, and A. Borning, "Value sensitive design and information systems," in *The Ethics of Information Technologies*, Routledge, 2020, pp. 289–313. Accessed: Dec. 27, 2023. [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.4324/9781003075011-21/value-sensitive-design-information-systems-peter-batya-friedman-kahn-alan-borning
[37] J.-H. Hoepman, "Privacy Design Strategies," in *ICT Systems Security and Privacy Protection*, vol. 428, N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, and T. Sans, Eds., in IFIP Advances in Information and Communication Technology, vol. 428. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 446–459. doi: 10.1007/978-3-642-55415-5_38.

[38] C. Adams, *Introduction to Privacy Enhancing Technologies: A Classification-Based Approach to Understanding PETs*. Springer Nature, 2021. Accessed: Jan. 01, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=lXdLEAAAQBAJ&oi=fnd&pg=PR7&dq=introduction+to+privacy+enhancing+technologies&ots=VLP4pO3bds&sig=JV6GFc75YbC91JSZAyZiRTlk-OQ

[39] P. M. Valkenburg, M. Krcmar, A. L. Peeters, and N. M. Marseille, "Devloping a Scale to Assess Three Styles of Television Mediation: Instructive Mediation, Restrictive Mediation, and Social Coviewing," *J Broad Elec Media*, vol. 43, p. 52, 1999.

[40] K. M. Collier *et al.*, "Does parental mediation of media influence child outcomes? A meta-analysis on media time, aggression, substance use, and sexual behavior.," *Dev. Psychol.*, vol. 52, no. 5, p. 798, 2016.

[41] P. Wisniewski, A. K. Ghosh, H. Xu, M. B. Rosson, and J. M. Carroll, "Parental Control vs. Teen Self-Regulation: Is there a middle ground for mobile online safety?," in *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, Portland Oregon USA: ACM, Feb. 2017, pp. 51–69. doi: 10.1145/2998181.2998352.

[42] R. Brito and P. Dias, "'Which apps are good for my children?': How the parents of young children select apps," *Int. J. Child-Comput. Interact.*, vol. 26, p. 100188, 2020.

[43] M. Mazmanian and S. Lanette, "'Okay, One More Episode': An Ethnography of Parenting in the Digital Age," in *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, Portland Oregon USA: ACM, Feb. 2017, pp. 2273–2286. doi: 10.1145/2998181.2998218.

[44] N. Sangal, D. Singhvi, M. Pharande, and D. Patole, "Teen-alyse: 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)*, IEEE, 2021, pp. 1–5. Accessed: Dec. 27, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9596148/

[45] M. Nouwen, M. Van Mechelen, and 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*, Boston Massachusetts: ACM, Jun. 2015, pp. 363–366. doi: 10.1145/2771839.2771917.

[46] M. Anderson, "Parents, teens and digital monitoring," 2016, Accessed: Dec. 27, 2023. [Online]. Available: https://policycommons.net/artifacts/618677/parents-teens-and-digital-monitoring/1599662/

[47] B. McNally *et al.*, "Co-designing Mobile Online Safety Applications with Children," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, Montreal QC Canada: ACM, Apr. 2018, pp. 1–9. doi: 10.1145/3173574.3174097.

[48] J. Y. Shin, M. Rheu, J. Huh-Yoo, and W. Peng, "Designing Technologies to Support Parent-Child Relationships: A Review of Current Findings and Suggestions for Future Directions," *Proc. ACM Hum.-Comput. Interact.*, vol. 5, no. CSCW2, pp. 1–31, Oct. 2021, doi: 10.1145/3479585.

[49] V. Rideout and M. B. Robb, "The Common Sense census: Media use by kids age zero to eight," *San Franc. CA Common Sense Media*, vol. 263, p. 283, 2017.

[50] J. Piaget, "Piaget's Theory," in *Piaget and His School*, B. Inhelder, H. H. Chipman, and C. Zwingmann, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 1976, pp. 11–23. doi: 10.1007/978-3-642-46323-5_2.

[51] S. Yadav, P. Chakraborty, P. Mittal, A. Kumar, and H. Gupta, “A Novel Technique to Detect Inappropriate Content Accessed by Children on Smartphone,” in *International Conference on Innovative Computing and Communications*, vol. 473, D. Gupta, A. Khanna, S. Bhattacharyya, A. E. Hassanien, S. Anand, and A. Jaiswal, Eds., in Lecture Notes in Networks and Systems, vol. 473. , Singapore: Springer Nature Singapore, 2023, pp. 91–105. doi: 10.1007/978-981-19-2821-5_8.

[52] A. K. Ghosh, K. Badillo-Urquiola, S. Guha, J. J. LaViola Jr, and P. J. Wisniewski, “Safety vs. Surveillance: What Children Have to Say about Mobile Apps for Parental Control,” in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, Montreal QC Canada: ACM, Apr. 2018, pp. 1–14. doi: 10.1145/3173574.3173698.

[53] A. K. Ghosh, K. Badillo-Urquiola, M. B. Rosson, H. Xu, J. M. Carroll, and 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*, Montreal QC Canada: ACM, Apr. 2018, pp. 1–14. doi: 10.1145/3173574.3173768.

[54] S. Kawas, N. S. Kuhn, K. Sorstokke, E. Bascom, A. Hiniker, and K. Davis, “When Screen Time Isn’t Screen Time: Tensions and Needs Between Tweens and Their Parents During Nature-Based Exploration,” in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, Yokohama Japan: ACM, May 2021, pp. 1–14. doi: 10.1145/3411764.3445142.

[55] J. H. Graafland, “New Technologies and 21st Century Children: Recent Trends and Outcomes. OECD Education Working Papers, No. 179.,” *OECD Publ.*, 2018, Accessed: Dec. 27, 2023. [Online]. Available: https://eric.ed.gov/?id=ED589953

[56] B. O’Neill, “Policy influences and country clusters: A comparative analysis of Internet safety policy implementation,” 2014, Accessed: Dec. 27, 2023. [Online]. Available: https://eprints.lse.ac.uk/57247/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_EU%20Kids%20Online_EU_Kids_Online_Report_PolicyInfluencesMay2014_Final.pdf

[57] “Digital Services Act - BIK Portal - BIK Community,” BIK Portal. Accessed: Dec. 27, 2023. [Online]. Available: https://www.betterinternetforkids.eu/policy/digitalservicesact

[58] “European strategy for a better Internet for kids (BIK+) - factsheet | Shaping Europe’s digital future.” Accessed: Dec. 27, 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/european-strategy-better-internet-kids-bik-factsheet

[59] “Special group on the EU Code of conduct on age-appropriate design | Shaping Europe’s digital future.” Accessed: Dec. 27, 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design

[60] “California Age Appropriate Design Code,” California Age Appropriate Design Code. Accessed: Dec. 27, 2023. [Online]. Available: https://californiaaadc.com/

[61] “California AB2273 | TrackBill.” Accessed: Dec. 27, 2023. [Online]. Available: https://trackbill.com/bill/california-assembly-bill-2273-the-california-age-appropriate-design-code-act/2228971/

[62] “coppa-2.0-one-pager-2023.pdf.” Accessed: Jan. 01, 2024. [Online]. Available: https://www.commonsensemedia.org/sites/default/files/featured-content/files/coppa-2.0-one-pager-2023.pdf

[63] E. J. [D-M. Sen. Markey, “Text - S.1418 - 118th Congress (2023-2024): Children and Teens’ Online Privacy Protection Act.” Accessed: Jan. 01, 2024. [Online]. Available: https://www.congress.gov/bill/118th-congress/senate-bill/1418/text

[64] M. Blumenthal, “IN THE SENATE OF THE UNITED STATES”.
[65] “kids_online_safety_act_one_pager.pdf.” Accessed: Jan. 01, 2024. [Online]. Available: https://www.young.senate.gov/imo/media/doc/kids_online_safety_act_one_pager.pdf
[66] “UK children and adults to be safer online as world-leading bill becomes law,” GOV.UK. Accessed: Dec. 27, 2023. [Online]. Available: https://www.gov.uk/government/news/uk-children-and-adults-to-be-safer-online-as-world-leading-bill-becomes-law
[67] “Learn about the Online Safety Act | eSafety Commissioner.” Accessed: Dec. 27, 2023. [Online]. Available: https://www.esafety.gov.au/newsroom/whats-on/online-safety-act
[68] “Public Bill (Senate) S-210 (44-1) - Third Reading - Protecting Young Persons from Exposure to Pornography Act - Parliament of Canada.” Accessed: Dec. 27, 2023. [Online]. Available: https://www.parl.ca/documentviewer/en/44-1/bill/S-210/third-reading
[69] L. Pasquale, P. Zippo, C. Curley, B. O’Neill, and M. Mongiello, “Digital Age of Consent and Age Verification: Can They Protect Children?,” *IEEE Softw.*, vol. 39, no. 3, pp. 50–57, May 2022, doi: 10.1109/MS.2020.3044872.
[70] S. Finnegan, “How Facebook Beat the Children’s Online Privacy Protection Act: A Look into the Continued Ineffectiveness of COPPA and How to Hold Social Media Sites Accountable in the Future,” *Seton Hall Rev*, vol. 50, p. 827, 2019.
[71] “Unduly restrictive?” Accessed: Dec. 27, 2023. [Online]. Available: https://nationalmagazine.ca/en-ca/articles/law/in-depth/2022/unduly-restrictive
[72] M. Geist, “Age Verification Requirements for Twitter or Website Blocking for Reddit?: My Appearance on Bill S-210 at the Senate Standing Committee on Legal and Constitutional Affairs - Michael Geist.” Accessed: Dec. 27, 2023. [Online]. Available: https://www.michaelgeist.ca/2022/02/age-verification-requirements-for-twitter-or-website-blocking-for-reddit-my-appearance-on-bill-s-210-at-the-senate-standing-committee-on-legal-and-constitutional-affairs/
[73] “The UK’s Online Safety Bill, explained - The Verge.” Accessed: Jan. 01, 2024. [Online]. Available: https://www.theverge.com/23708180/united-kingdom-online-safety-bill-explainer-legal-pornography-age-checks
[74] “Kids’ Privacy (COPPA) | Federal Trade Commission.” Accessed: Dec. 27, 2023. [Online]. Available: https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/kids-privacy-coppa
[75] “Film Ratings,” Motion Picture Association. Accessed: Jan. 01, 2024. [Online]. Available: https://www.motionpictures.org/film-ratings/
[76] “History.” Accessed: Jan. 01, 2024. [Online]. Available: https://www.filmratings.com/History
[77] “Our History,” ESRB Ratings. Accessed: Dec. 27, 2023. [Online]. Available: https://www.esrb.org/history/
[78] “About the International Age Rating Coalition | IARC.” Accessed: Jan. 01, 2024. [Online]. Available: https://www.globalratings.com/about.aspx
[79] M. G. Noll and C. Meinel, “Web page classification: An exploratory study of the usage of Internet content rating systems,” *LIASIT-Luxemb. Int. Adv. Stud. Inf. Technol. Luxemb.*, vol. 14, 2005, Accessed: Dec. 27, 2023. [Online]. Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=478fc294bc8b7efd71e4a873997542ea8840cbec
[80] C. T. Marsden, *Internet co-regulation: European law, regulatory governance and legitimacy in cyberspace*. Cambridge University Press, 2011. Accessed: Dec. 27, 2023. [Online]. Available:

https://books.google.com/books?hl=en&lr=&id=dbX_LJoh270C&oi=fnd&pg=PR1&dq=Marsden,+Christopher+T.+Internet+co-regulation:+European+law,+regulatory+governance+and+legitimacy+in+cyberspace&ots=Pbi_jnaySM&sig=JJvZyvRcyhnNe32RveloMBdhW8c

[81] "Home - age-label.com." Accessed: Dec. 27, 2023. [Online]. Available: https://age-label.com/

[82] "Age Labels Data Model Community Group." Accessed: Dec. 27, 2023. [Online]. Available: https://www.w3.org/community/agelabels/

[83] G. Wang, J. Zhao, M. Van Kleek, and N. Shadbolt, "12 Ways to Empower: Designing for Children's Digital Autonomy," in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, Hamburg Germany: ACM, Apr. 2023, pp. 1–27. doi: 10.1145/3544548.3580935.

[84] K. Badillo-Urquiola, D. Smriti, B. McNally, E. Golub, E. Bonsignore, and P. J. Wisniewski, "Stranger Danger!: Social Media App Features Co-designed with Children to Keep Them Safe Online," in *Proceedings of the 18th ACM International Conference on Interaction Design and Children*, Boise ID USA: ACM, Jun. 2019, pp. 394–406. doi: 10.1145/3311927.3323133.

[85] "Glossary | CSRC." Accessed: Dec. 27, 2023. [Online]. Available: https://csrc.nist.gov/glossary

[86] A. F. Westin, "Privacy and freedom," *Wash. Lee Law Rev.*, vol. 25, no. 1, p. 166, 1968.

[87] D. J. Solove, "A taxonomy of privacy," *U Pa Rev*, vol. 154, p. 477, 2005.

[88] P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. F. Cranor, "Exploring How Privacy and Security Factor into IoT Device Purchase Behavior," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, Glasgow Scotland Uk: ACM, May 2019, pp. 1–12. doi: 10.1145/3290605.3300764.

[89] Y. Huang, B. Obada-Obieh, and K. (Kosta) Beznosov, "Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, Honolulu HI USA: ACM, Apr. 2020, pp. 1–13. doi: 10.1145/3313831.3376529.

[90] H. J. Smith, S. J. Milberg, and S. J. Burke, "Information privacy: Measuring individuals' concerns about organizational practices," *MIS Q.*, pp. 167–196, 1996.

[91] C. Weir, B. Hermann, and S. Fahl, "From needs to actions to secure apps? the effect of requirements and developer practices on app security," in *29th USENIX security symposium (USENIX security 20)*, 2020, pp. 289–305. Accessed: Dec. 27, 2023. [Online]. Available: https://www.usenix.org/conference/usenixsecurity20/presentation/weir

[92] M. Tahaei, K. Vaniea, and N. Saphra, "Understanding Privacy-Related Questions on Stack Overflow," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, Honolulu HI USA: ACM, Apr. 2020, pp. 1–14. doi: 10.1145/3313831.3376768.

[93] R. Wash, "Folk models of home computer security," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, Redmond Washington USA: ACM, Jul. 2010, pp. 1–16. doi: 10.1145/1837110.1837125.

[94] J. Zhao *et al.*, "`I make up a silly name': Understanding Children's Perception of Privacy Risks Online," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, Glasgow Scotland Uk: ACM, May 2019, pp. 1–13. doi: 10.1145/3290605.3300336.

[95] S. Maqsood and S. Chiasson, "'They think it's totally fine to talk to somebody on the internet they don't know': Teachers' perceptions and mitigation strategies of tweens' online risks," in

Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama Japan: ACM, May 2021, pp. 1–17. doi: 10.1145/3411764.3445224.
[96] U. Bronfenbrenner, "Ecological models of human development," *Int. Encycl. Educ.*, vol. 3, no. 2, pp. 37–43, 1994.
[97] L. Sweeney, "k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY," *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, vol. 10, no. 05, pp. 557–570, Oct. 2002, doi: 10.1142/S0218488502001648.
[98] "web_almanac_2022_en.pdf." Accessed: Dec. 27, 2023. [Online]. Available: https://cdn.httparchive.org/almanac/ebooks/web_almanac_2022_en.pdf
[99] M. Luo, B. Feng, L. Lu, E. Kirda, and K. Ren, "On the Complexity of the Web's PKI: Evaluating Certificate Validation of Mobile Browsers," *IEEE Trans. Dependable Secure Comput.*, 2023, Accessed: Dec. 27, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10066507/?casa_token=i85tcZ_9RVAAAAAA:khOKGmcWHonLx0ziSwBsljGbbNqlO_30YtKyleJs5cmF5GFBcc9wWIJXnyZpqtVhKFzAeCYWefk
[100] A. S. Wazan, R. Laborde, D. W. Chadwick, F. Barrere, and A. Benzekri, "Tls connection validation by web browsers: Why do web browsers still not agree?," in *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, IEEE, 2017, pp. 665–674. Accessed: Dec. 27, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8029674/?casa_token=ZVkUuLzeRusAAAAA:3pMAF3HBGoePMI1qyTpnqHaK0ajqOI31tqHvH_CRxF5KRhYmzSB_dQlWrJsDJEOcBFZkPe3i3R0
[101] S. Boeyen, S. Santesson, T. Polk, R. Housley, S. Farrell, and D. Cooper, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," Internet Engineering Task Force, Request for Comments RFC 5280, May 2008. doi: 10.17487/RFC5280.
[102] A. Jøsang, I. G. Pedersen, and D. Povey, "PKI Seeks a Trusting Relationship," in *Information Security and Privacy*, vol. 1841, E. P. Dawson, A. Clark, and C. Boyd, Eds., in Lecture Notes in Computer Science, vol. 1841. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 191–205. doi: 10.1007/10718964_16.
[103] "B.3. Standard X.509 v3 Certificate Extension Reference Red Hat Certificate System 9 | Red Hat Customer Portal." Accessed: Dec. 27, 2023. [Online]. Available: https://access.redhat.com/documentation/en-us/red_hat_certificate_system/9/html/administration_guide/standard_x.509_v3_certificate_extensions
[104] A. K. Ghosh, C. E. Hughes, and P. J. Wisniewski, "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*, Honolulu HI USA: ACM, Apr. 2020, pp. 1–14. doi: 10.1145/3313831.3376747.
[105] M. Kumar, V. Dwivedi, A. Sanyal, P. Bhatt, and R. Koshariya, "Parental Security Control: A tool for monitoring and securing children's online activities.," in *2021 Thirteenth International Conference on Contemporary Computing (IC3-2021)*, Noida India: ACM, Aug. 2021, pp. 469–474. doi: 10.1145/3474124.3474196.
[106] W. Fuertes, K. Quimbiulco, F. Galárraga, and J. L. García-Dorado, "On the development of advanced parental control tools," in *2015 1st International Conference on Software Security and Assurance (ICSSA)*, IEEE, 2015, pp. 1–6. Accessed: Dec. 27, 2023. [Online]. Available:

https://ieeexplore.ieee.org/abstract/document/7812938/?casa_token=mtmTdKdwuxQAAAAA:n0AHHrobGWs_tPmjcl7KnYSGEHWFxinH107vj7MBdn6cbaf8WjN_0tuo_Aq4ogx2jZ9tn7pVsQQ
[107] "Top 10 Shopify Age Verification Apps [December, 2023]," Acquire Convert. Accessed: Dec. 27, 2023. [Online]. Available: https://acquireconvert.com/best-shopify-apps/shopify-age-verification-app/
[108] CDC, "Child Development Positive Parenting Tips | CDC," Centers for Disease Control and Prevention. Accessed: Dec. 27, 2023. [Online]. Available: https://www.cdc.gov/ncbddd/childdevelopment/positiveparenting/index.html
[109] "chrome.storage | API | Chrome for Developers." Accessed: Dec. 27, 2023. [Online]. Available: https://developer.chrome.com/docs/extensions/reference/api/storage#storage_areas
[110] S. Santesson, *RFC 4680: TLS Handshake Message for Supplemental Data*. USA: RFC Editor, 2006.
[111] A. King, "Certainly Something (Certificate Viewer)." Dec. 11, 2023. Accessed: Jan. 01, 2024. [Online]. Available: https://github.com/april/certainly-something
[112] A. K. Ghosh, "A Value Sensitive Design Approach to Adolescent Mobile Online Safety," 2018, Accessed: Jan. 01, 2024. [Online]. Available: https://stars.library.ucf.edu/etd/6053/
[113] P. Wisniewski, H. Xu, M. B. Rosson, and J. M. Carroll, "Parents Just Don't Understand: Why Teens Don't Talk to Parents about Their Online Risk Experiences," in *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, Portland Oregon USA: ACM, Feb. 2017, pp. 523–540. doi: 10.1145/2998181.2998236.
[114] L. Steinberg, S. D. Lamborn, S. M. Dornbusch, and N. Darling, "Impact of Parenting Practices on Adolescent Achievement: Authoritative Parenting, School Involvement, and Encouragement to Succeed," *Child Dev.*, vol. 63, no. 5, p. 1266, Oct. 1992, doi: 10.2307/1131532.
[115] P. Wisniewski *et al.*, "Resilience Mitigates the Negative Effects of Adolescent Internet Addiction and Online Risk Exposure," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, Seoul Republic of Korea: ACM, Apr. 2015, pp. 4029–4038. doi: 10.1145/2702123.2702240.
[116] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Q.*, pp. 319–340, 1989.
[117] J. Lazar, J. H. Feng, and H. Hochheiser, *Research methods in human-computer interaction*. Morgan Kaufmann, 2017. Accessed: Jan. 02, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=hbkxDQAAQBAJ&oi=fnd&pg=PP1&dq=analyzing+qualitative+data+research+methods+in+human+computer+interaction&ots=Sr133g12cO&sig=edX0DEhbU4OqqSPMztDFv-2Kr1g
[118] H. Sharp, *Interaction design*. John Wiley & Sons, 2003.
[119] H. Castillo-Parra, J. A. Zeladita-Huaman, L. Cárdenas-Niño, R. Zegarra-Chapoñán, J. M. Cuba-Sancho, and G. I. Morán-Paredes, "Validation of the Steinberg Parenting Styles Scale in Peruvian adolescents," *Int. J. Psychol. Res.*, vol. 15, no. 2, pp. 68–76, 2022.
[120] "Use parental controls on your child's iPhone, iPad, and iPod touch," Apple Support. Accessed: Dec. 27, 2023. [Online]. Available: https://support.apple.com/en-ca/HT201304

[121] “Legal - Family Privacy Disclosure for Children - Apple,” Apple Legal. Accessed: Dec. 27, 2023. [Online]. Available: https://www.apple.com/legal/privacy/en-ww/parent-disclosure/
[122] “Manage devices, apps & screen time - Google For Families Help.” Accessed: Dec. 27, 2023. [Online]. Available: https://support.google.com/families/topic/7336331?hl=en&ref_topic=6149867&sjid=7331857171781758115-NC
[123] “How Google Accounts work when children turn 13 (or the applicable age in your country) - Google For Families Help.” Accessed: Dec. 27, 2023. [Online]. Available: https://support.google.com/families/answer/7106787?hl=en#zippy=%2Ccontinue-their-current-parental-supervision-settings
[124] “Getting started with Microsoft Family Safety - Microsoft Support.” Accessed: Dec. 27, 2023. [Online]. Available: https://support.microsoft.com/en-us/account-billing/getting-started-with-microsoft-family-safety-b6280c9d-38d7-82ff-0e4f-a6cb7e659344
[125] “Important info for parents about YouTube Kids - YouTube For Families Help.” Accessed: Dec. 27, 2023. [Online]. Available: https://support.google.com/youtubekids/answer/6130561?hl=en#zippy=%2Chow-are-videos-available-in-youtube-kids-selected%2Cwhat-parental-controls-are-available-in-youtube-kids
[126] “Parents’ Ultimate Guide to YouTube Kids | Common Sense Media.” Accessed: Dec. 27, 2023. [Online]. Available: https://www.commonsensemedia.org/articles/parents-ultimate-guide-to-youtube-kids
[127] “Netflix wants to help parents connect with their kids by explaining what they’re watching - The Verge.” Accessed: Dec. 27, 2023. [Online]. Available: https://www.theverge.com/2020/12/8/22163863/netflix-family-profile-kids-activity-report-data-movies-tv-shows-individual
[128] “Parental controls on Netflix,” Help Center. Accessed: Dec. 27, 2023. [Online]. Available: https://help.netflix.com/en/node/264
[129] “Parents, Safety, and Moderation – Roblox Support.” Accessed: Dec. 27, 2023. [Online]. Available: https://en.help.roblox.com/hc/en-us/categories/200213830-Parents-Safety-and-Moderation
[130] “Parents’ Ultimate Guide to Roblox | Common Sense Media.” Accessed: Dec. 27, 2023. [Online]. Available: https://www.commonsensemedia.org/articles/parents-ultimate-guide-to-roblox

Appendix A

X.509 Certification Signing Request Configuration with Age Rating

The below example shows a CSR configuration for a site with age rating ‘P’.

```
oid_section             = new_oids

# To use this configuration file with the "-extfile" option of the
# "openssl x509" utility, name here the section containing the
# X.509v3 extensions to use:
# extensions            =
# (Alternatively, use a configuration file that has only
# X.509v3 extensions in its main [= default] section.)

[ new_oids ]
kidsAssProp = 1.3.6.1.4.1.60933.1

[ req ]
default_bits      = 2048
distinguished_name = req_distinguished_name
req_extensions     = v3_ext

[ req_distinguished_name ]
countryName               = CA
stateOrProvinceName       = ON
localityName              = Locality Name (eg, city)
organizationName          = PROKIDS
commonName                = PROKIDS
CN = prokids.ca
```

[seq_sect]

[v3_ext]
subjectAltName = @alt_names
keyUsage=nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage=serverAuth
kidsAssProp = ASN1:UTF8String:P

[alt_names]
DNS.1 = prokids.ca
DNS.2 = www.prokids.ca

Appendix B

Host Server Configuration And Certificates

The tested content servers were hosted on HostPapa, a Canadian web hosting site and self-signed X.509 certificates were installed.

Age rating	**Domain name**	**Site purpose**	**Age Rating on Firefox Certificate Viewer**
P (0-5)	prokids.ca	Day care website	Assessed Kids Rating Rating Preschool (0-5, preliterate and early literacy)
E (6-9)	kidstreaming.ca	Video streaming for young children	Assessed Kids Rating Rating Elementary (6-9, core primary school years)
T (10-12)	teenlearning.ca	Educational site	Assessed Kids Rating Rating Transition (10-12)
ET (13-15)	earlyteengames.ca	Game site tweens and teens.	Assessed Kids Rating Rating Early Teen (13-15)
MT (16-17)	midteenblogger.ca	Blogger site for midteens and up.	Assessed Kids Rating Rating Mid Teen (16-17, approaching adulthood)

Appendix C

Firefox Certificate Viewer Update

The codes for original Firefox browser certificate viewer was updated to translate the new extension field.

The updates were found in this repository:

- Original certificate viewer repo: https://github.com/april/certainly-something
- KidsPro certificate viewer repo: https://github.com/jdaws9499/certainlysomething

The updates are mainly to add the new OID translation and allowing the new extension checking.

- I18n String.js

```
  '1.3.6.1.4.1.60933.1': {
    name: {
      short: 'Kids Rating',
      long: 'Assessed Kids Rating'
    }
  }
},
```

```
kidsRatings: {
  'P': 'Preschool (0-5, preliterate and early literacy)',
  'E': 'Elementary (6-9, core primary school years)',
  'T': 'Transition (10-12)',
  'ET':'Early Teen (13-15)',
  'MT': 'Mid Teen (16-17, approaching adulthood)',
},
```

- Der.js

```
// get KidsPro assigned rating
let kpr = getX509Ext(x509.extensions,'1.3.6.1.4.1.60933.1').extnID;
if (kpr) {
  console.log('found kpr');
  let pValue = getX509Ext(x509.extensions,'1.3.6.1.4.1.60933.1').extnValue.valueBlock.value[0].valueBlock.value
  kpr = {
    critical: criticalExtensions.includes('1.3.6.1.4.1.60933.1'),
    requred: false,
    value: pValue,
    rating: strings.kidsRatings[pValue]
  }
}
```

```
export const parse = async (certificate) => {
  const supportedExtensions = [
    '1.3.6.1.4.1.311.20.2',      // microsoft certificate type
    '1.3.6.1.4.1.311.21.2',      // microsoft certificate previous hash
    '1.3.6.1.4.1.311.21.7',      // microsoft certificate template
    '1.3.6.1.4.1.311.21.1',     // microsoft certification authority renewal
    '1.3.6.1.4.1.311.21.10',     // microsoft certificate policies
    '1.3.6.1.4.1.11129.2.4.2',   // embedded scts
    '1.3.6.1.5.5.7.1.1',         // authority info access
    '1.3.6.1.5.5.7.1.24',        // ocsp stapling
    '1.3.101.77',                // ct redaction - deprecated and not displayed
    '2.5.29.14',                 // subject key identifier
    '2.5.29.15',                 // key usages
    '2.5.29.17',                 // subject alt names
    '2.5.29.19',                 // basic constraints
    '2.5.29.31',                 // crl points
    '2.5.29.32',                 // certificate policies
    '2.5.29.35',                 // authority key identifier
    '2.5.29.37',                 // extended key usage
    '1.3.6.1.4.1.60933.1', //Added kidsPro Rating  change
  ];
```

Appendix D

ProKids Tool Codes

ProKids mediation tool was implemented as a Firefox browser add-on.

- Repo: https://github.com/jdaws9499/kidspro-npm

- Manifest.json

```
{
  "manifest_version": 2,
  "name": "Kidspro Npm",
  "version": "0.1.0",
  "description": "Guides kids to browse Internet more safely by tracking
kids appropriate ratings on visiting websites",
  "author":
  "page_action": {
    "default_icon": "icons/dyno_icon.png",
    "default_title": "kidspro Npm",
    "default_popup": "popup_success.html",
    "show_matches": [
      "https://*/*"
    ]
  },
  "browser_action": {
    "default_title": "my favorite color"
  },
  "icons": {
    "16": "icons/abc_icon.png",
    "32": "icons/dyno_icon.png"
  },
  "background": {
    "scripts": [
      "background.js"
    ]
  },
  "options_ui": {
    "page": "options.html",
    "browser_style": true,
```

```
    "open_in_tab": true
  },
  "permissions": [
    "activeTab",
    "storage",
    "notifications",
    "menus",
    "contextMenus",
    "webRequest",
    "webRequestBlocking",
    "scripting",
    "<all_urls>"
  ],
  "content_scripts": [
    {
      "matches": [
        "<all_urls>"
      ],
      "run_at": "document_idle",
      "js": [
        "contentScript.js"
      ]
    }
  ],
  "browser_specific_settings": {
    "gecko": {
      "id": "kidspro-npm@mozilla.org",
      "strict_min_version": "57.0a1"
    }
  },
  "web_accessible_resources": [
    "blocked.html"
  ]
}
```

- Kidspro-npm@mozilla.org.json

```
{
    "name":  "kidspro-npm@mozilla.org",
    "description": "ignored",
    "type": "storage",
```

```
    "data": {
      "kidsProUser": "user related...",
      "kidsProAdmin": "admin related...."
    }
}
```

- Options.js – user settings

```
/******/ (() => { // webpackBootstrap
var __webpack_exports__ = {};
/*!**********************!*\
  !*** ./src/options.js ***!
  \**********************/
//'use strict';

//import './options.css';

let adminPass = '';

const allowedForAll = [
    'https://protectkidsonline.ca',
    'https://www.cybertip.ca'
];

function promptAdminPassword(action) {

    browser.windows.create(
        {
            url: 'prompt.html?action=' + encodeURIComponent(action),
            type: 'popup',
            height: 400,
            width: 600
        }
    );
}

function createAdminPassword() {
    browser.windows.create(
        {
            url: 'createPassword.html',
            type: 'popup',
```

```
            height: 400,
            width: 600
        }
    );
}

async function saveOptionsWithPrompt(e) {
    //createAdminPassword();
    promptAdminPassword("saveOptions");
    e.preventDefault();
}

function sendResetCacheMessage(message) {
    chrome.runtime.sendMessage(
        {
            type: 'RESET_CACHE',
            reason: message
        },
        (response) => {
            console.log(response.message);
        }
    );

}

async function saveOptions() {
    console.log('bday typed value: ' +
document.querySelector("#bdate").value);
    let birthdate = Date.parse(document.querySelector("#bdate").value);
    console.log('birthdate:' + birthdate);
    // send background to reset caches.
    sendResetCacheMessage('settings update');
    console.log('nickanme' + document.querySelector("#nickname").value);
    browser.storage.sync.set({
        kidsProUser: {
            preference: {
                nickname: document.querySelector("#nickname").value,
                bdate: document.querySelector("#bdate").value,
                rating: getRating(birthdate),
                allowed: {
                    urls: document.querySelector("#allowedUrls").value ||
"[]"
```

```
                },
                blocked: {
                    urls: document.querySelector("#blockedUrls").value ||
"[]"
                },
                schedules: document.querySelector("#schedules").value ||
"[]"
            },
            admin: {
                password: document.querySelector("#password").value || ""
            },
            logs: document.querySelector("#logs").value || "[]"
        }
    });
    location.reload();
}

async function resetOptionsWithPrompt(e) {
    promptAdminPassword("resetOptions");
    e.preventDefault();
}

function resetOptions() {
    console.log('reset options');
    browser.storage.sync.set({
        kidsProUser: {
            preference: {
                nickname: "",
                bdate: "",
                rating: "",
                allowed: {
                    urls: "[]"
                },
                blocked: {
                    urls: "[]"
                },
                schedules: "[]"
            },
            admin: {
                password: document.querySelector("#password").value || ""
            },
            logs: document.querySelector("#logs").value || "[]"
```

```
        }
    });
    location.reload();
}

function displayAllowedForAll(itemsStr) {
    let items = itemsStr;
    let html = "";
    if (items) {
        for (let i = 0; i < items.length; i++) {
            html += "<li class=\"list-group-item\">"
            html += items[i];
            html += "</li>";
        }
    }
    console.log('display - ' + html);
    document.querySelector("#displayAllowedForAll").innerHTML = html;
}

function displayAllowedItems(itemsStr) {
    console.log('value' + itemsStr);
    console.log('display' +
document.querySelector("#displayAllowed").value);

    let items = itemsStr;
    let html = "";
    if (items) {
        for (let i = 0; i < items.length; i++) {
            html += "<tr>"
            html += "<td>" + (i + 1) + "</td>"
            html += "<td>" + items[i] + "</td>";
        }
    }
    console.log('display - ' + html);
    document.querySelector("#displayAllowed").innerHTML = html;
}

function displayBlockedItems(itemsStr) {
    console.log('value' + itemsStr);
    console.log('display' +
document.querySelector("#displayBlocked").value);
```

```
    let items = itemsStr;
    let html = "";
    if (items) {
        for (let i = 0; i < items.length; i++) {
            //html += "<li class=\"list-group-item\">"
            html += "<tr>"
            html += "<td>" + (i + 1) + "</td>"
            html += "<td>" + items[i] + "</td>";
            //html += "</li>";
        }
    }
    console.log('display - ' + html);
    document.querySelector("#displayBlocked").innerHTML = html;
}

function isSiteAllowed(siteAccess) {
    return (siteAccess === 'A' || siteAccess === 'AW');
}



function getBlockedReason(siteAccess) {
    let reason = 'not known.';
    if (siteAccess === 'B') {
        reason = 'blocked with age rating limit.';
    } else if (siteAccess === 'BB') {
        reason = 'block websites list';
    } else if (siteAccess === 'BBB') {
        reason = 'outside the browse schedule';
    } else if (siteAccess === 'AW') {
        reason = 'allowed with age rating limit.'
    }
    return reason;
}

function displayLogs(logs) {
    console.log('displayLogs - ' + logs);
    let html = "";
    let items = logs;
    if (items) {
        let options = {
            year: "numeric",
```

```
            month: "numeric",
            day: "numeric",
            hour: "numeric",
            minute: "numeric",
            second: "numeric",
            hour12: true
        };
        for (let i = 0; i < items.length; i++) {
            let color = "list-group-item-info";
            let siteAccess = items[i].siteAccess;
            if (siteAccess === 'AW') {
                color = "list-group-item-warning";
            } else if (siteAccess === 'BB' || siteAccess === 'B') {
                color = "list-group-item-danger";
            }
            let logItem = items[i];
            let isAllowed = isSiteAllowed(logItem.siteAccess);
            if (isAllowed) {
                html += "<tr class=\"table-warning\">";
            } else {
                html += "<tr>";
            }

            html += "<td>" + new Intl.DateTimeFormat("en-CA",
options).format(new Date(items[i].time)) + "</td>";
            html += "<td>" + logItem.url.substring(0, 50) + "</td>";
            html += "<td>" + getBlockedReason(logItem.siteAccess) +
"</td>";
            html += "<td>";
            //if (items[i].numOfTries && items[i].numOfTries > 1 ) {
            html += logItem.numOfTries;
            //}
            html += "</td>";
            html += "</tr>";
        }
    }
    document.querySelector("#displayLogs").innerHTML = html;
}

function displaySchedules(schedules) {
    console.log('displaySchedules - ') + schedules;
    let html = "";
```

```
    let items = schedules; // string to json object
    if (items) {
        for (let i = 0; i < items.length; i++) {
            html += "<tr>";
            html += "<td>" + getDayOfWeek(items[i].dayId) + "</td>";
            html += "<td>" + items[i].from + "</td>";
            html += "<td>" + items[i].to + "</td>";
            html += "</tr>";
        }
    }
    document.querySelector("#displaySchedule").innerHTML = html;

}

function getDayOfWeek(dayId) {
    if (dayId) {
        if (dayId === 'day1') {
            return "Monday";
        } else if (dayId === 'day2') {
            return "Tuesday";
        } else if (dayId === 'day3') {
            return "Wednesday";
        } else if (dayId === 'day4') {
            return "Thursday";
        } else if (dayId === 'day5') {
            return "Friday";
        } else if (dayId === 'day6') {
            return "Saturday";
        } else if (dayId === 'day0') {
            return "Sunday";
        }
    } else {
        return 'NA';
    }
}

async function addScheduleWithPrompt(e) {
    promptAdminPassword("addSchedule");
    e.preventDefault();
}

function clearNewScheduleField() {
```

```
    document.querySelector("#daySelect").selected = false;

    document.querySelector("#fromTime").value = "";
    document.querySelector("#toTime").value = "";
}

function addCheckedDay(day, fromTime, toTime, days) {
    days.push({ dayId: day, from: fromTime, to: toTime });
    //return days;
}

async function addSchedule() {
    console.log('addSchedule + ' +
document.querySelector("#daySelect").value);
    let days = [];
    let fromTime = document.querySelector("#fromTime").value;
    let toTime = document.querySelector("#toTime").value;
    let selectedDay = document.querySelector("#daySelect").value;

    console.log(selectedDay + ': from - ' + fromTime + ' to ' + toTime);

    addCheckedDay(selectedDay, fromTime, toTime, days);
    let schedules = JSON.parse(document.querySelector("#schedules").value
|| "[]"); // array strings to array object
    console.log('adding - ' + JSON.stringify(days));
    schedules = schedules.concat(days);
    let sorted = await schedules.sort((a, b) => {
        //1. Check day of the week
        if (a.dayId < b.dayId) {
            return -1;
        } else if (a.dayId > b.dayId) {
            return 1;
        } else {
            //2. from time
            if (a.from < b.from) {
                return -1;
            } else if (a.from > b.from) {
                return 1;
            } else {
                //3. to time
                if (a.to < b.to) {
                    return -1;
```

```
                } else if (a.to > b.to) {
                    return 1;
                } else {
                    return 0;
                }
            }
            return 0;
        }
    });

    if (sorted) {
        document.querySelector("#schedules").value =
JSON.stringify(sorted);
        console.log('schedules -' +
document.querySelector("#schedules").value);
        clearNewScheduleField();
        saveOptions();
    }
}

async function clearSchedulesWithPrompt(e) {
    promptAdminPassword("clearSchedules");
    e.preventDefault();
}

async function clearSchedules() {
    console.log('clearSchedules');
    document.querySelector("#schedules").value = "[]";
    saveOptions();
}

async function clearLogsWithPrompt(e) {
    promptAdminPassword("clearLogs");
    e.preventDefault();
}

async function clearLogs() {
    console.log('clearLogs');
    document.querySelector("#logs").value = "[]";
    saveOptions();
}
```

```
async function addAllowItemWithPrompt(e) {
    promptAdminPassword("addAllowItem");
    e.preventDefault();
}

function addAllowItem() {
    console.log('addAllowItem');
    let newItem = document.querySelector("#newAllowItem").value;
    let urls = JSON.parse(document.querySelector("#allowedUrls").value ||
"[]");
    urls.push(newItem);
    //document.querySelector("output[name='allowedUrls']").value =
JSON.stringify(urls);
    document.querySelector("#allowedUrls").value = JSON.stringify(urls);
    document.querySelector("#newAllowItem").value = "";
    //displayAllowedItems(JSON.stringify(urls));
    saveOptions();
}

async function clearAllowItemsWithPrompt(e) {
    promptAdminPassword("clearAllowItems");
    e.preventDefault();
}

async function clearAllowItems() {
    console.log('clearAllowItems');
    document.querySelector("#allowedUrls").value = "[]";
    saveOptions();
}

async function addBlockItemWithPrompt(e) {
    promptAdminPassword("addBlockItem");
    e.preventDefault();
}

function addBlockItem() {
    console.log('addBlockItem');
    let newItem = document.querySelector("#newBlockItem").value;
```

```
    let urls = JSON.parse(document.querySelector("#blockedUrls").value ||
"[]");
    urls.push(newItem);
    //displayBlockedItems(JSON.stringify(urls));
    document.querySelector("#blockedUrls").value = JSON.stringify(urls);
    document.querySelector("#newBlockItem").value = "";
    saveOptions();
}

async function clearBlockItemsWithPrompt(e) {
    promptAdminPassword("clearBlockItems");
    e.preventDefault();
}

async function clearBlockItems() {
    console.log('clearBlockItems');
    document.querySelector("#blockedUrls").value = "[]";
    saveOptions();
}


function getRating(birthday) {
    let age = calculateAge(birthday);
    console.log('age: ' + age);
    let rating = 'NA';
    if (age > -1) {
        if (age <= 5) {
            rating = 'P';
        } else if (age <= 9) {
            rating = 'E';
        } else if (age <= 12) {
            rating = 'T';
        } else if (age <= 15) {
            rating = 'ET';
        } else if (age <= 17) {
            rating = 'MT';
        }
        console.log('rating: ' + rating);
        return rating;
    } else {
        return 'NA';
```

```
        //throw new Error('cannot get rating from birthday - ' +
birthday);
    }
}

function calculateAge(birthday) { // birthday is a date
    if (birthday) {
        var ageDifMs = Date.now() - birthday;
        var ageDate = new Date(ageDifMs); // miliseconds from epoch
        return Math.abs(ageDate.getUTCFullYear() - 1970);
    } else {
        return -1;
    }
}

function getMinimumDate() {
    let minDate = new Date();
    let day = minDate.getDate();
    let month = minDate.getMonth();
    if (month < 10) {
        month = '0' + month;
    }
    let year = minDate.getFullYear() - 18;
    minDate = year + '-' + month + '-' + day
    console.log('17 yr old birthdate: ' + minDate)
    return minDate;
}

function adminLogout() {
    console.log('adminLogout');
}


function restoreOptions() {
    try {
        console.log('restoreOptions');
        //let storage = browser.storage.managed;
        let storageItem = browser.storage.managed.get('kidsProUser');
        storageItem.then((res) => {
            document.querySelector("#managed-bdate").innerText =
res.kidsProUser.bdate;
        });
```

```
        let userData = browser.storage.sync.get('kidsProUser');
        userData.then((res) => {
            console.log('data ' + JSON.stringify(res.kidsProUser));
            document.querySelector("#nickname").value =
res.kidsProUser.preference.nickname || 'Not Set';
            document.querySelector("#bdate").value =
res.kidsProUser.preference.bdate || getMinimumDate;
            document.querySelector("output[name='rating']").value =
res.kidsProUser.preference.rating || 'NA';
            if (res.kidsProUser.preference.blocked) {
                document.querySelector("output[name='blockedUrls']").value
= res.kidsProUser.preference.blocked.urls;
                displayBlockedItems(JSON.parse(res.kidsProUser.preference.
blocked.urls));
            }
            if (res.kidsProUser.preference.allowed) {
                document.querySelector("output[name='allowedUrls']").value
= res.kidsProUser.preference.allowed.urls;
                displayAllowedItems(JSON.parse(res.kidsProUser.preference.
allowed.urls));
            }
            //displayAllowedForAll(allowedForAll);
            if (res.kidsProUser.preference.schedules) {
                document.querySelector("output[name='schedules']").value =
res.kidsProUser.preference.schedules;
                displaySchedules(JSON.parse(res.kidsProUser.preference.sch
edules));
            }

            document.querySelector("output[name='password'").value =
res.kidsProUser.admin.password;

            if (res.kidsProUser.logs) {
                document.querySelector("output[name='logs']").value =
res.kidsProUser.logs;
                displayLogs(JSON.parse(res.kidsProUser.logs));
            }
        });

    } catch (error) {
        console.error(error);
```

```
    }
}

browser.runtime.onMessage.addListener((request, sender, sendResponse) => {
    console.log('options.js received a message- ' +
JSON.stringify(request));

    if (request.type === 'action') {
        if (request.message === 'saveOptions') {
            saveOptions();
        } else if (request.message === 'resetOptions') {
            resetOptions();
        } else if (request.message === 'addAllowItem') {
            addAllowItem();
        } else if (request.message === 'addBlockItem') {
            addBlockItem();
        } else if (request.message === 'addSchedule') {
            addSchedule();
        } else if (request.message === 'clearSchedules') {
            clearSchedules();
        } else if (request.message === 'clearAllowItems') {
            clearAllowItems();
        } else if (request.message === 'clearBlockItems') {
            clearBlockItems();
        } else if (request.message === 'clearLogs') {
            clearLogs();
        } else if (request.message === 'restoreOptions') {
            restoreOptions();
        }
    }
});

document.addEventListener('DOMContentLoaded', restoreOptions);
window.addEventListener("beforeunload", adminLogout);
document.querySelector("#save").addEventListener("click",
saveOptionsWithPrompt);
document.querySelector("#reset").addEventListener("click",
resetOptionsWithPrompt);
document.querySelector("#addAllow").addEventListener("click",
addAllowItemWithPrompt);
document.querySelector("#addBlock").addEventListener("click",
addBlockItemWithPrompt);
```

```
document.querySelector("#clearAllowItems").addEventListener("click",
clearAllowItemsWithPrompt);
document.querySelector("#clearBlockItems").addEventListener("click",
clearBlockItemsWithPrompt);
document.querySelector("#addSchedule").addEventListener("click",
addScheduleWithPrompt);
document.querySelector("#clearSchedules").addEventListener("click",
clearSchedulesWithPrompt);
document.querySelector("#clearLogItems").addEventListener("click",
clearLogsWithPrompt);




/******/ })()
;
//# sourceMappingURL=options.js.map
```

Background.js – verifying certificates

```
import { Certificate } from 'pkijs';
import * as asn1js from 'asn1js';
const NodeCache = require("node-cache");
const bcrypt = require("bcryptjs");
const ratingCache = new NodeCache();


const allowedForAll = [
  'https://protectkidsonline.ca',
  'https://www.cybertip.ca',
  'https://cybertip.ca'
];
//'use strict';

// With background scripts you can communicate with popup
// and contentScript files.
// For more information on background script,
// See https://developer.chrome.com/extensions/background_pages

/**
 * @param {*} extensions
```

```
 * @param {*} id
 * @returns
 */
function getX509Ext(extensions, id) {
  for (var extension in extensions) {
    if (extensions[extension].extnID === id) {
      return extensions[extension];
    }
  }
}

let safe = true;
let block = false;
const ratings = [
  'P', // 0-5
  'E', // 6-9
  'T', // 10-12
  'ET', // 13-15
  'MT']; // 16-17

const accessLevel = [
  'A', // Allow
  'AW', // Allowed with warning for teens
  'B',  // Blocked age rating
  'BB', // Blocked list
  'BBB' // Blocked hours
]

async function validateSite(details) {
  const preference = getPreference();
  const siteRating = await getCertificateRating(details);

  let ratingMatched = true;
  let allowed = false;
  let blocked = false;
  let siteUrl = new URL(details.url);

  console.log('siteUrl origin - ' + siteUrl.origin);
  let siteAccess = 'A';

  if (allowedForAll.includes(siteUrl.origin) || siteRating) {
    console.log('**siteRating: ' + siteRating);
```

```
    if (!allowedForAll.includes(siteUrl.origin) && preference.rating &&
ratings.indexOf(preference.rating) > -1) {
      ratingMatched = ratings.indexOf(siteRating) > -1 &&
(ratings.indexOf(siteRating) <= ratings.indexOf(preference.rating));
      if (!ratingMatched) {
        if (preference.rating === 'P' || preference.rating === 'E')
{ // || siteRating === 'NA'
          siteAccess = 'B';
        } else {
          console.log('site access AW');
          siteAccess = 'AW'; // not the raiting but allowed with
warning
        }
      }
    }

    if (preference.allowedUrls) { // overrides everything above
      allowed = preference.allowedUrls.indexOf(siteUrl.origin) > -1;
      if (allowed) {
        siteAccess = 'A';
      }
    }

    if (preference.blockedUrls) { // overrides everything above
      blocked = preference.blockedUrls.indexOf(siteUrl.origin) > -1;
      if (blocked) {
        siteAccess = 'BB';
      }
    }
    console.log('siteAccess - ' + siteAccess);
    ratingCache.set(siteUrl.origin, siteAccess, 10000);

  }

}

//browser.runtime.onMessage.addListener(handleSiteAccess)

async function getCertificateRating(details) {
  try {
    console.log('newcert - ' + JSON.stringify(details));
```

```
    let securityInfo = await browser.webRequest.getSecurityInfo(
      details.requestId,
      { "certificateChain": true, rawDER: true }
    );
    if (securityInfo) {
      let cert = securityInfo.certificates[0];
      //console.log('certificate - ' + JSON.stringify(cert));
      let certificateChain = new Uint8Array(cert.rawDER).buffer;
      let asn1 = asn1js.fromBER(certificateChain);

      let x509 = await new Certificate({ schema: asn1.result });
      if (x509) {
        x509 = x509.toJSON();
        //console.log('x509 in pkijs - ' + x509);
        console.log('extensions - ' + JSON.stringify(x509.extensions));
        /*let san = getX509Ext(x509.extensions,
'2.5.29.17').parsedValue;
        if (san && san.hasOwnProperty('altNames')) {
          //console.log('*Subject Alt Names: ' + JSON.stringify(san));
        }*/
        let kidsRatingValue = getX509Ext(x509.extensions,
"1.3.6.1.4.1.60933.1");
        if (kidsRatingValue) {
          return kidsRatingValue.parsedValue.valueBlock.value;
        } else {
          return "NA";
        }
      }
    }

  } catch (error) {
    console.error(error);
    throw error;
  }
};

async function getCurrentTab() {
  let queryOptions = { active: true, lastFocusedWindow: true };
  // `tab` will either be a `tabs.Tab` instance or `undefined`.
  let [tab] = await chrome.tabs.query(queryOptions);
  return tab;
}
```

```
function getPreference() {
  let preference = ratingCache.get('preference');
  if (!preference) {
    preference = parsePreference();
  }
  console.log('pref:' + JSON.stringify(preference));
  return preference;
}

async function getAdminPassword() {
  let userData = await browser.storage.sync.get('kidsProUser');
  let pass = '';
  if (userData) {
    pass = userData.kidsProUser.admin.password;
  }
  return pass;
}

async function addLogItem(logItem) {
  try {
    let userData = await browser.storage.sync.get('kidsProUser');
    if (userData) {
      console.log('saving log item...' + JSON.stringify(logItem));
      console.log('data ' + JSON.stringify(userData.kidsProUser));
      let pref = userData.kidsProUser.preference;
      let admin = userData.kidsProUser.admin;
      let logs = JSON.parse(userData.kidsProUser.logs || "[]");
      if (logs.length > 0) {
        let lastItem = logs[logs.length - 1];
        if (lastItem.url === logItem.url) {
          // don't log the same site multiple times if it's recent one.
          //let item = { time: new Date(), url: url, siteAccess:
siteAccess };
          if (lastItem.numOfTries) {
            logItem.numOfTries = lastItem.numOfTries + 1;
          } else {
            logItem.numOfTries = 2;
          }
          logs.pop();
        }
      }
```

```
      logs.push(logItem);
      if (logs > 50) {
        logs.shift(); // keep the length to 50.
      }
      let saved = browser.storage.sync.set({
        kidsProUser: {
          preference: pref,
          admin: admin,
          logs: JSON.stringify(logs)
        }
      });
    }
  } catch (error) {
    console.error(error);
  }
}

async function saveAdminPassword(password) {
  try {
    let hashValue = await bcrypt.hash(password, 8);
    let userData = await browser.storage.sync.get('kidsProUser');

    if (hashValue && userData) {
      //
      console.log('saving hash..' + hashValue);
      let pref = userData.kidsProUser.preference;
      let logs = userData.kidsProUser.logs;
      let saved = browser.storage.sync.set({
        kidsProUser: {
          preference: pref,
          admin: {
            password: hashValue
          },
          logs: logs
        }
      });
      return true;

    }
  } catch (error) {
    console.error(error);
    return false;
```

```
  }
}

async function parsePreference() {
  let userData = await browser.storage.sync.get('kidsProUser');
  let pref = {};
  if (userData) {
    pref.rating = userData.kidsProUser.preference.rating;
    if (userData.kidsProUser.preference.allowed) {
      pref.allowedUrls = userData.kidsProUser.preference.allowed.urls;
    }
    if (userData.kidsProUser.preference.blocked) {
      pref.blockedUrls = userData.kidsProUser.preference.blocked.urls;
    }
    if (userData.kidsProUser.preference.schedules) {
      pref.schedules = userData.kidsProUser.preference.schedules;
    }
  }
  console.log('parsed preference');
  ratingCache.set('preference', pref);
  return pref;
}

async function logRedirect(url, siteAccess) {
  if (siteAccess === 'B' || siteAccess === 'BB' || siteAccess ===
'BBB') { // only log when kids violated knowingly...
    logAccessViolated(url, siteAccess);
  }
}

async function logAccessViolated(url, siteAccess) {
  let item = { time: new Date(), url: url, siteAccess: siteAccess,
numOfTries: 1 };
  addLogItem(item);
}

function redirect(tabId, url, siteAccess) {
  // log redirect
  logRedirect(url, siteAccess);
```

```
  const redirectUrl = browser.runtime.getURL('blocked.html') + '?url='
+ encodeURIComponent(url) + '?access=' +
encodeURIComponent(siteAccess);
  // siteRating
  // p1: outside approved hours BBB
  // p2: blocked site BB
  // p3: age rating B

  chrome.tabs.update(tabId, {
    url: redirectUrl
  });
}

function verifyAllowedSchedules() {
  console.log('verifyAllowedSchedules');
  const preference = getPreference();

  const schedules = JSON.parse(preference.schedules || "[]");
  if (schedules.length === 0) { // allow always lest defined
    console.log('allow always');
    return true;
  }
  const now = new Date();
  const today = now.getDay();

  const currentHour = now.getHours();

  const currentMinute = now.getMinutes();
  console.log('today is Day +' + today);
  for (const schedule of schedules) {
    if (schedule.dayId === 'day' + today) { // day5 = Friday

      if (schedule.from < schedule.to) {
        console.log('from is smaller');
        if (schedule.from <= currentHour + ':' + currentMinute &&
schedule.to > currentHour + ':' + currentMinute) {
          // match allow
          console.log('match allow - ' + schedule);
          return true;
        }
      }
    }
```

```
  }
  console.log('schedule not allowed');
  return false;
}

browser.tabs.onUpdated.addListener(function (tabId, changeInfo) {
  if (!changeInfo.url || changeInfo.url.startsWith("moz-extension:"))
{ // redirecting
    return;
  }

  const originUrl = new URL(changeInfo.url).origin;
  console.log('changeInfo.url.origin: ' + originUrl);

  // check time
  let allow = verifyAllowedSchedules();
  if (allow === false) {
    console.log('schedule allowed? ' + allow + ' redirect');
    redirect(tabId, changeInfo.url, 'BBB'); // BBB blocked by schedules
  } else {

    // check site rating

    let siteAccess = ratingCache.get(originUrl);
    console.log('siteacess ' + siteAccess);
    if (siteAccess) {

      console.log('found siteAccess: ' + siteAccess);

      //TODO cache site rating also
      if (siteAccess === 'A') {
        browser.pageAction.setIcon({
          tabId: tabId,
          path: "icons/dyno_icon.png"
        });
        browser.pageAction.setTitle({
          tabId: tabId,
          title: "kidspro Npm"
        });
      }

      if (siteAccess === 'AW') {
```

```
        logAccessViolated(changeInfo.url, siteAccess);

        browser.pageAction.setIcon({
          tabId: tabId,
          path: "icons/info_icon.png"
        });
        browser.pageAction.setTitle({
          tabId: tabId,
          title: "kidspro Npm - warning"
        });
        browser.pageAction.setPopup({
          tabId: tabId,
          popup: "popup_warning.html"
        });

        browser.notifications.create({
          iconUrl: "icons/fox.jpg",
          type: "basic",
          title: "KidsPro alert",
          message: 'Hi you are visiting a website you are not supposed
to.',
          contextMessage: 'this message is...'
        });
      }

      if (siteAccess === 'B' || siteAccess === 'BB') { ///BBB is
already redirectd
        redirect(tabId, changeInfo.url, siteAccess);
      }
    }
  }
  console.log('exit');
});

browser.runtime.onInstalled.addListener(() => {
  // tracking badge text ON or OFF
  console.log('new install');
  /*browser.pageAction.setBadgeText({
      text: "SAFE",
  });*/
  /*browser.notifications.create('above rating', {
    type: "basic",
```

```
    title: "KidsPro alert",
    message: 'Hi you are visiting a website you are supposed to.'
  });*/

  parsePreference();

});

browser.webRequest.onHeadersReceived.addListener(
  details => {
    validateSite(details);
  },
  { urls: ["<all_urls>"], types: ["main_frame"] },
  ["blocking"]
);

browser.webRequest.onErrorOccurred.addListener(
  details => {
    // eventually we will be able to consume these details, but for now
we can only
    // disable the icon
    // consume(details);
    if (details.type === 'main_frame' && details.documentUrl ===
undefined) {
      console.log('error happend' + JSON.stringify(details));
      //icon.update(details.tabId, 'http');
    }
  },
  { urls: ['<all_urls>'] }
);

browser.runtime.onMessage.addListener((request, sender, sendResponse)
=> {
  console.log('backgrounds.js received a message- ' +
JSON.stringify(request));
  if (request.type === 'GREETINGS') {
    const message = `Hi ${sender.tab ? 'Con' : 'Pop'
      }, my name is Bac. I am from Background. It's great to hear from
you.`;

    // Log message coming from the `request` parameter
    console.log(request.payload.message);
```

```
    // Send a response message
    sendResponse({
      message,
    });
    return true;
  } else if (request.type ==='RESET_CACHE') {
    console.log('reset cache..');
    ratingCache = new NodeCache();
    sendResponse({ message: "reset cache success" });
    return true;
  } else if (request.type === 'verifyPassword') {
    const getP = getAdminPassword();
    getP.then(function (password) {
      console.log('password - ' + password);
      const getV = bcrypt.compare(request.password, password);
      getV.then(function (result) {
        console.log('result - ' + result);
        if (result === true) {
          // ok.
          console.log('match!');
          sendResponse({ message: "success" });
        } else {
          console.log('fail!');
          sendResponse({ message: "fail" });
        }
      });
    });

    return true;
  } else if (request.type === 'storePassword') {
    const saveP = saveAdminPassword(request.password);
    saveP.then(function (result) {
      console.log('save result - ' + result);
      sendResponse({ message: "success" });
    });
    return true;
  }
});

function handleClick(e) {
  browser.runtime.openOptionsPage();
}
```

```
function handleStorageChange(storage) {
  parsePreference();
}

browser.browserAction.onClicked.addListener(handleClick);
browser.storage.onChanged.addListener(handleStorageChange);
```

- popup_warning.html – providing warning popup

```
<!DOCTYPE html>
<html lang="en">

<head>
  <meta charset="utf-8">
  <title>KidsPro - Popup</title>
  <link rel="shortcut icon" href="icons/abc_icon.ico">
  <link rel="stylesheet" href="./popup.css" />
  <link
href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.m
in.css" rel="stylesheet" />
  <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-
icons@1.11.1/font/bootstrap-icons.css">
</head>

<body>
  <body style="width: 15rem;height: 17rem;">
    <div class="row">
      <div class="card text-bg-warning">

        <div class="card-header">
          KidsPro
        </div>
        <div class="card-body">
          <h5 class="card-title">We think this site may have harmful
contents. You can ask any question you have or get help if you have
experienced something bad.</h5>
          <a href="https://www.cybertip.ca/en/report/" class="btn btn-
primary"><i class="bi bi-question-circle-fill"></i> Ask</a>
```

```
          <a href="https://protectkidsonline.ca/app/en/" class="btn
btn-secondary"><i class="bi bi-info-circle-fill"></i> Help</a>
        </div>
      </div>
    </div>

  <script src="popup.js"></script>

  <!--
      This HTML file opens when you click on icon from the toolbar.

      To begin the development, run `npm run watch`.
      To create a production bundle, use `npm run build`.
    -->
</body>

</html>
```

- popup_success.html – providing friendly message

```
<!DOCTYPE html>
<html lang="en">

<head>
  <meta charset="utf-8">
  <title>KidsPro - Popup</title>
  <link rel="shortcut icon" href="icons/abc_icon.ico">
  <link rel="stylesheet" href="./popup.css" />
  <link
href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.m
in.css" rel="stylesheet" />
  <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-
icons@1.11.1/font/bootstrap-icons.css">
</head>

<body style="width: 15rem;height: 13rem;">
  <div class="row">
    <div class="card col-12 border-success">

      <div class="card-header bg-transparent border-success">
        KidsPro
```

```
      </div>
      <div class="card-body text-success">
        <h5 class="card-title">We think this site is safe. But do you
think otherwise? Please ask.</h5>
        <a href="https://www.cybertip.ca/en/report/" class="btn btn-
success"><i class="bi bi-question-circle-fill"></i> Ask</a>
      </div>
    </div>
  </div>

  <script src="popup.js"></script>

  <!--
      This HTML file opens when you click on icon from the toolbar.

      To begin the development, run `npm run watch`.
      To create a production bundle, use `npm run build`.
    -->
</body>

</html>
```

User Study Approval

25/09/2023

Université d'Ottawa
Bureau d'éthique et d'intégrité de la recherche

University of Ottawa
Office of Research Ethics and Integrity

CERTIFICAT D'APPROBATION ÉTHIQUE | CERTIFICATE OF ETHICS APPROVAL

Numéro du dossier / Ethics File Number	H-09-23-9574
Titre du projet / Project Title	Start building safe network for kids
Type de projet / Project Type	Thèse de maîtrise / Master's thesis
Statut du projet / Project Status	Approuvé / Approved
Date d'approbation (jj/mm/aaaa) / Approval Date (dd/mm/yyyy)	25/09/2023
Date d'expiration (jj/mm/aaaa) / Expiry Date (dd/mm/yyyy)	24/09/2024

Équipe de recherche / Research Team

Chercheur / Researcher	Affiliation	Role
Juehee DAWSON	École de science informatique et de génie électrique / School of Electrical Engineering and Computer Science	Chercheur Principal / Principal Investigator
Carlisle ADAMS	École de science informatique et de génie électrique / School of Electrical Engineering and Computer Science	Superviseur / Supervisor

Conditions spéciales ou commentaires / Special conditions or comments

Appendix E

User Study - Recruitment Form

Our research group at the School of Electrical Engineering at the University of Ottawa is currently conducting a research study. The purpose of this study is to introduce a new prototype system to provide children with age-appropriate content with reduced security and privacy risks while reducing gaps between recent policies, companies' implementation efforts around age-appropriate content, and shortcomings of existing parental control apps.

Your participation in the study will consist of a pre-survey, a demo followed by an interview.

During a confidential online survey, participants will be asked questions about their online parenting strategies. The survey will take about 10 minutes to complete. Participants will then be asked to watch a demo of the tool features either online via Zoom or in-person for about 15 minutes. A follow-up interview will be taken place either online via Zoom or in-person, participants will be asked questions about their perception of the system. The interview takes approximately 20-30 minutes to complete. In-person sessions will be held in a university of Ottawa lab.

There will be a small store gift card of $10 for every participation. To be eligible, participants should:

- Be over 18 years old, and
- Have one or more children who are under 18 years old.

Participants will be selected on a first-come, first-served basis. If you are interested, please email Juehee Dawson for more details on participating.

Ethical Review

This research has been reviewed and cleared by the Research Ethics Board (REB) of University of Ottawa.

Date of Clearance: September 25, 2023

Ethics Clearance for the Collection of Data Expires: September 24, 2024

Office of Research Ethics and Integrity: ethics@uottawa.ca

Appendix F

User Study – Consent Form

Title of the study: ProKids

Invitation to Participate: I am invited to participate in the above-mentioned research study conducted by Juehee Dawson in the context of a Master's thesis, under the supervision of Dr. Adams.

Purpose of the Study: The purpose of the study is to introduce a new prototype system to provide children with age-appropriate content with reduced security and privacy risks while reducing gaps in between recent policies, companies' implementation efforts around age-appropriate content, and shortcomings of existing parental control applications.

Participation: The research study involves participating in a user study consisting of a pre-survey, a demo followed by an interview. The online survey regarding parenting strategies will take about 10 minutes, I will observe the demo on the features of the parental control tool for about 15 minutes. During a follow-up interview of 20-30 minutes, I will answer questions about my experience with the system, my perception of age-appropriate contents and my experience with parental control tool. I am aware that the interview will be audio-recorded.

Risks: There are no known risks associated with this study. During the study, I will be able to skip questions if I choose. I have the right to withdraw from the interview at any time. If I withdraw from the session, my data will be deleted and not used for analysis. Data collected during the session will be saved with a file name as an anonymous pseudonym that has no connection with any personally identifiable data. All responses will be confidential. After data collection is complete, data will be stored on a password-protected computer that uses hard-disk encryption, associated with an anonymous pseudonym. Only researchers directly involved in the research will have access to the study area.

Benefits: My participation in this study will help improve children's online browsing experience.

Confidentiality and Privacy I have received assurance from the researchers that the information I will share will remain strictly confidential. I understand that the contents will be used only for the study and that my identity will be protected by keeping the data with an unidentifiable pseudonym. If I choose to participate online, in order to minimize the risk of security breaches and to help ensure my confidentiality, it is recommended that I use standard safety measures, such as signing out of logged in websites and applications, closing my browser, and locking my device when I am no longer using it/when I have completed the study.

Conservation of Data: The interview will be audio-recorded and safely kept on an encrypted and password-protected computer for five years. Access will be restricted to those researchers directly involved with the research.

Compensation: I will be compensated with a $10 Starbucks store gift card. I will still receive the compensation if I choose to withdraw from the study.

Voluntary Participation: I am under no obligation to participate and if I choose to participate, I can withdraw from the study at any time and/or refuse to answer any questions, without suffering any negative consequences. If I choose to withdraw, all data gathered until the time of withdrawal will be removed from the dataset and not used in the study.

If I have any questions about the study, I may contact the researcher or their supervisor. If I have any questions regarding the ethical conduct of this study, I may contact the Office of Research Ethics and Integrity via email (ethics@uottawa.ca) or telephone (613-562-5387).

It is recommended that I keep a copy of this consent form for my records.

Acceptance: By signing my name below, I agree to participate in this research study.

Participant's name: _____ Date: _____
Participant's signature: _____ Date: _____
Researcher's signature: _____ Date: _____

Appendix G

Interview Questionnaire

Q1. Do you use or have you used a parental control appliance such as Qustodio, Norton Family, Circle Home Plus, Kaspersky Safe Kids, Google Family Link, Apple Parental control, Microsoft Family Safety?

Q2. Of the tools you've tried or heard of, which tool did you like better and why?

Q3. Of the tools you have used or heard of, which one do you think would be more effective in protecting teens and children from encountering content risks? Why?

Q4. Which tool would be more respectful of a child's personal privacy?

Q5. Which tool, if any, would be the best fit for the needs of your family? Why? If none would be a best fit, why?

Q6. In terms of parental monitoring to ensure your child's safety, what do you think are the most important considerations for doing this in your family?

Q7. Overall impression of the ProKids tool

Q8. Which features did you like? Why?

Q9. Which features did you not like? Why?

Q10. Any suggestions to improve the tool?

Appendix H

Pre-Survey Questionnaire

Demographic Questionnaire

1. What is your gender? (Female, Male, Non-binary, Prefer not to say)
2. How old are you? (under 24 years old, 25-34, 35-44, 45-54, 55 years old or older)
3. How old is your child or how old are your children if you have more than one?
4. What ethnicity do you identify with most? (White/Caucasian, Black/African Canadian, Hispanic/Latino, Asian, First Nation, Inuit, and Métis, Other)
5. What is your highest level of education achieved? (Less than high school, Completed high school, Some college, Completed college degree, Some trade/technical training, Completed trade/technical training, Some university, Bachelor's degree, Master's degree, Doctorate degree)

Children's Online Activities Questionnaire

How often do your children spend time online? Please answer per child (under 18) for the following questions. It can be a combination of time spent alone or with family.

6. How often does your oldest child watch videos online? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)
7. How often does your second child watch videos online? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)
8. How often does your third child watch videos online? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)
9. How often does your oldest child use social media? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)

10. How often does your second child use social media? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)

11. How often does your third child use social media? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)

12. How often does your oldest child send and receive text messages via social media or any other apps supporting texts (including texting to parents)? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)

13. How often does your second child send and receive text messages via social media or any other apps supporting texts (including texting to parents)? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)

14. How often does your third child send and receive text messages via social media or any other apps supporting texts (including texting to parents)? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)

15. How often does your oldest child send and receive media files (e.g., pictures, videos)? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)

16. How often does your second child send and receive media files (e.g., pictures, videos)? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)

17. How often does your third child send and receive media files (e.g., pictures, videos)? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)

18. How often does your oldest child shop online (e.g., purchase apps, games and other items)? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)

19. How often does your second child shop online (e.g., purchase apps, games and other items)? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)

20. How often does your third child shop online (e.g., purchase apps, games and other items)? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)

21. How often does your oldest child play games online? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)

22. How often does your second child play games online? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)

23. How often does your third child play games online? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other) How often does your oldest child search or browse websites?

24. How often does your oldest child search or browse websites? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)

25. How often does your second child search or browse websites? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)

26. How often does your third child search or browse websites? (I don't know, Daily or almost daily, Weekly or weekends only, Monthly, Never, Other)

Family Communication (Wisniewski et al., 2017)

27. Please answer the following questions based on your own experience. (Likert)

- I initiate family meetings to discuss problems or issues my children might be dealing with being online. (Strongly agree, Somewhat agree, Neutral, Somewhat disagree, Strongly disagree)

- I talk to my child about family rules about what he/she does online. (Strongly agree, Somewhat agree, Neutral, Somewhat disagree, Strongly disagree)

- I talk to my child about how to resist peer pressure to do inappropriate things online. (Strongly agree, Somewhat agree, Neutral, Somewhat disagree, Strongly disagree)

- I talk to my child about how to engage safely about how to engage safely with others while him/her online. (Strongly agree, Somewhat agree, Neutral, Somewhat disagree, Strongly disagree)

Parenting Styles (Steinberg et al., 1992)

28. Please respond to the following statements with the answer that best describes the relationship you have with your child.

(My child can count on me to help him/her out, if he/she has some kind of problem, I tell my child that you shouldn't argue with adults, I push my child to do his/her best in whatever he/she does, I tell my child that he/she should give in on arguments rather than make people angry, I keep pushing my child to think independently, When my child gets a poor grade in school, I make his/her life miserable, I help my child with his/her schoolwork, I tell my child that my ideas are correct and that he/she should not question them, When I want my child to do something, I explain why, When my child gets a poor grade in school, I encourage him/her to try harder, I let my child make his/her own plans for things he/she wants to do, I know who my child's friends are, I act cold and unfriendly if my child does something I don't like, I spend time just talking with my child, When my child gets a poor grade in school, I make him/her feel guilty, My family does things for fun together, I won't let my child do things with me when he/she does something I don't like.)

29. Please respond based on how much you try to know each of the following about your children's activities. (Likert)

- Where your child goes at night? (Extremely likely, Somewhat likely, Neutral, Somewhat unlikely, Extremely unlikely)
- What your child does with his/her free time? (Extremely likely, Somewhat likely, Neutral, Somewhat unlikely, Extremely unlikely)
- Where your child is most afternoons after schools? (Extremely likely, Somewhat likely, Neutral, Somewhat unlikely, Extremely unlikely)

30. Please respond based on how much you really know each of the following about your children's activities. (Likert)

- Where your child goes at night? (Extremely likely, Somewhat likely, Neutral, Somewhat unlikely, Extremely unlikely)
- What your child does with his/her free time? (Extremely likely, Somewhat likely, Neutral, Somewhat unlikely, Extremely unlikely) Where your child is most afternoons after schools?
- Where your child is most afternoons after schools? (Extremely likely, Somewhat likely, Neutral, Somewhat unlikely, Extremely unlikely)

<u>Online Risk Experience (Wisniewski et al., 2015)</u>

31. Based on your knowledge of your child's experience within the past year, please indicate whether he/she was victimized online in the following ways. (Likert)

- Online interactions between your child and others that involved someone treating another person in a mean or hurtful way, making rude or threatening comments,

spreading untrue rumors, harassing, or otherwise trying to "cyberbully" another person. (Yes, No, I don’t know)

- Online interactions between your child and others that involved exchanging sexual messages (i.e. sexting), sexually suggestive text-based messages or revealing/naked photos, or arranging to meet someone first met online for an offline romantic encounter. (Yes, No, I don’t know)
- Online interactions between your child and others that involved sharing personal or sensitive information either without the owner's consent or that otherwise breached someone's personal privacy. (Yes, No, I don’t know)

Appendix I

Exit Survey Questionnaire

Technology Acceptance Model Variables (Davis, 1989)

Please specify whether you disagree or agree with the following statements. (Likert)

- Using the system would help me spend less time in keeping my child safe online. (Strongly agree, Somewhat agree, Neutral, Somewhat disagree, Strongly disagree)
- Using the system would improve my performance to keep my child safe online. (Strongly agree, Somewhat agree, Neutral, Somewhat disagree, Strongly disagree)
- Using the system would increase my ability to keep my child safe online. (Strongly agree, Somewhat agree, Neutral, Somewhat disagree, Strongly disagree)
- Using the system would enhance my effectiveness on keeping my child safe online. (Strongly agree, Somewhat agree, Neutral, Somewhat disagree, Strongly disagree)
- Using the system would make it easier to keep my child safe online. (Strongly agree, Somewhat agree, Neutral, Somewhat disagree, Strongly disagree)
- I would find the system useful in keeping my child safe online. (Strongly agree, Somewhat agree, Neutral, Somewhat disagree, Strongly disagree)