# Leveraging Cybersecurity Principles in Parental Controls

Matthew Howell

College of Technology, Wilmington University

## Author Note

I have no conflict of interest to disclose.

Correspondence concerning this paper should be addressed to Matt Howell via email at research@hcf.solutions.

**Abstract**

This paper identifies parental control features described by caregivers and researchers in light of cybersecurity principles. A literature review was performed for research describing technical parental mediation and parental controls. Twenty-three features were identified, ranging from setting time limits and restricting content to approving social media posts and detecting malicious activity. These features were mapped onto NIST's Cybersecurity Framework 2.0 resulting in risk and outcome descriptions that would fulfill the features described in the literature. These descriptions can be used to develop new parental control systems, audit existing systems, and evaluate compensating controls in network configurations to provide technical mediation.

*Keywords*: parental control, technical mediation, parental mediation, cybersecurity framework, adolescent online safety

**Contents**

## Introduction

Parental mediation is the body of techniques and technologies used by parents and caregivers to manage their children's media consumption based on the parent's family values (Wisniewski et al., 2017). Parental controls is the subset of parental mediation that utilizes hardware and software to accomplish technical mediation. Parental mediation has been a research topic since the rise of digital media and has recently focused on the complete development of the child and the parent-child dyad as it relates to communication and collaboration. However, recent research in the parental controls subtopic is lacking. Technology available to consumers and families has continued to progress while products available are falling behind and contemporary concerns are not being addressed at a comparative rate. Gaps in parental controls would best be addressed by applying contemporary cybersecurity principles and methods to both research and application (i.e. product development). If technical options do not evolve to keep pace with the ever-improving digital landscape, caregivers and children will be left with outdated and inferior choices to express and encounter family values in digital life.

### Background

Digital parental controls can be found in very early online services and communities (Assie, 2024). As internet usage grew and devices to access content diversified, parental controls moved into its own field of research and commercial space. It has been a field of academic study since the 2000s (e.g. Thierer, 2009). As Thierer described, during this time frame parental controls addressed not only internet usage, but risks in other technologies such as television, movies, music, and video game content. As the balance of media consumption shifted from physical devices like CDs and video game cartridges to the internet and online streaming platforms the demand for parental controls moved to internet-based systems and applications.

The effects of this shift to internet-dominated media consumption are beginning to be observed and researched. An increase in anxiety and depression among adolescents correlates

to the rise of their mobile phone and social media usage (Haidt, 2024). Current research in the field include topics like social media (e.g. Sevilla-Fernández et al., 2025), mobile devices (e.g. Elmogy & Elkhowiter, 2017), collaboration (e.g. Akter et al., 2022), and privacy (e.g. Duchaussoy, 2020).

**Not Cybersecurity Aware**

Modern parental controls must protect systems with various devices and connected to a multitude of networks (some under the caregiver's control and others not). Some content is traditional internet traffic through browsers while other content is opaque as it flows through apps on special purpose operating systems. Children become proficient in current technology faster than the caregivers who manage their devices. Those children are also encouraged to learn how to read and develop computer code and are required to maximize the internet for research. This creates opportunities to challenge and circumvent parental controls. As caregivers utilize dialog-based active mediation (Chen & Chng, 2016) they may need their parental control technology to identify patterns of activity and behavior then deliver alerts and reports in response.

While these challenges may be novel and even overwhelming to an amateur technologist implementing a home network, all of these challenges are common to cybersecurity professionals implementing public and private sector networks (e.g. Chandramouli, 2022). Common solutions or current threats being addressed in the cybersecurity space include zero trust and bring-your-own-device endpoint protection, integrating traditional and cloud-based traffic monitoring and filtering, threat modeling and addressing insider threats, and security event monitoring and reporting.

Parental control technology currently available is inadequate for the needs of caregivers and children. Existing products focus on reduced costs, ease of deployment, and/or ease of use, while failing to evaluate current needs and addressing modern parental control challenges. The technology to address most (if not all) parental control features exists in the professional

information security realm but these features have not been cataloged, mapped, and described in a manner sufficient to develop a modern parental control system.

### *Inferior Products If Left Unaddressed*

Many parental control solutions exist but they are segmented and time consuming to implement (Stouffer, 2022). Without a unifying structure to parental controls, the barrier to entry of implementation will grow and parental controls will lose effectiveness. The unified solutions that do exist are often constrained by cost and delivered as a function of convenience. Solutions constrained by cost will be unable to implement features that keep pace with evolving technologies. Solutions bound by their convenience of implementation will lack complex or standalone features, making for a mediocre experience.

Inferior products also impact children. As children grow into adulthood some negatively reflect on their restrictive mediation, some recount a desire for more parental controls, and others claim to be unaffected by restrictive controls (Skiera, 2024). Poor parental controls will decrease positive and neutral outlooks on restrictions and increase negative experiences among all children. If parental controls do not keep pace with technology both parents and children will have a frustrating experience of parental controls.

## Statement of the Problem

This paper attempts to determine if modern cybersecurity principles can sufficiently define parental control features. In order to define features based on cybersecurity principles, a catalog of desired features must be made. Once a catalog of features is developed, each one can be classified and addressed. For all features that can be addressed through technical mediation (i.e. parental controls), a mapping can then be made from the desired feature to a corresponding cybersecurity-aware framework outcome. This outcome can be used to define requirements familiar to public and private information security systems. Documented, commonplace, and accepted solutions in a professional system can then be used to implement the feature. This paper documents and maps parental control features to the framework

described below allowing future researchers and designers to define necessary requirements and develop modern parental control solutions.

## Framework and Overview

The NIST Cybersecurity Framework 2.0 (CSF; National Institute of Standards and Technology, 2024) is used to evaluate literature, determine features, highlight gaps, and identify accepted solutions in the cybersecurity space. Other frameworks were considered, such as CISv8 (Center for Internet Security, Inc., 2021) and NIST SP 800-53 (Joint Task Force Interagency Working Group, 2020), but rejected due to their prescriptive nature since they were too specific to public and commercial cybersecurity applications and not easily adaptable to parental controls.

Cybersecurity Framework, version 2.0 specifically, defines six core functions that can be used to manage cybersecurity risk. The Identify function describes identifying cybersecurity risks a target faces. CSF's Protect function covers preventative measures to address identified risks. The Detect function describes abilities that identify and analyze risks actively being exploited. The Respond function covers features that are activated in response to a detected incident. The Recover function includes activities after an incident response to restore the system to original operations. Finally, the Govern function informs all other functions and encompasses the risk management strategy, policies, and implementation (National Institute of Standards and Technology, 2024).

While the parental control system itself represents the Govern function, all other functions can be correlated to parental control features, risks the features address, or implementation needs of the features. The literature review is used to identify parental control features, risks, and implementation requirements. These in turn can be addressed by (mapped to) one or more CSF functions (Identify, Protect, Detect, Respond, or Recover).

## Research Method

As previously stated, this problem is addressed through a literature review performed using peer-reviewed articles and conference proceedings. Database searches target Google Scholar, ProQuest, and EBSCO online platforms. Articles were then limited to the past five years (i.e. since January 2020) due to the speed of technological advancements and shifting caregiving needs in response to the COVID-19 pandemic.

Search terms and keywords included “parental control systems methods,” “parental control technology”, and “parental mediation software.” Where supported, the term “parental control” was queried as an exact phrase (e.g. "parental control” AND systems AND methods). Sources were evaluated based on recency and relevance. Findings were organized by parental control feature and evaluated against the CSF framework as described above.

### *Case Studies*

In addition to academic literature, the problem of inadequate parental control features has been observed firsthand. Anecdotal accounts are presented here as informal case studies to illustrate the real world need for this research, though no academic case studies were discovered or used as part of the research.

Dustin Kirkland, an information security executive, set up parental controls in his family’s network and devices. In 2024 his daughters, subjects of the parental controls and age 11 and 12 at the time, found ways to circumvent parental controls and gain unauthorized access (Burch, 2025). The security failure was due to software bugs in two separate Google products (Kirkland, 2025). Primary parental control features were identified and implemented by the parent but failed due to software bugs. If secondary control features were identified and implemented (e.g. behavior logging of browsing content, or access logging of elevated privileges) the failure may have been identified earlier.

The most common use case of technology among minors (and of parental controls), however, does not require the caregiver to be a technology executive. Journalist Joel Burgess

recounts events leading up to giving his 11 year old son an iPhone and the concerns and challenges that followed (Burgess, 2025). His hesitancy revolved around the potential of the internet and social media to influence and damage children who are still developing mentally. Parental controls were available and he implemented some controls, but the software proved to be confusing to manage. Burgess also describes a situation where his son circumvented controls and accessed YouTube. Though the incident was unintentional it highlights the mismatch of parental control features between what is readily available and what is needed.

## Literature Review

While parental controls in media have been developed and studied since the 2000s, recent research has focused on the human-computer interaction of parental controls and active mediation (e.g. Sweigart et al., 2025). No systematic review of technical features required by parental controls could be found from the past 5 years. Features necessary are mentioned in literature to varying degrees of detail and rarely centralized. Literature pertaining to parental controls and technical mediation was reviewed and features desired, used, and evaluated by caregivers, teenagers, and researchers were identified as described in Research Method.

### Mediation Scope

As summarized by Sevilla-Fernández et al. (2025), there are many taxonomies defined to describe parental controls. At the highest level, parental mediation pertains to the entire effort (principles, policies, techniques, etc.) used by caregivers to safely present digital media to adolescence in their care (Livingstone et al., 2017). Livingstone & Helsper (2008) break parental mediation into restrictive mediation (rule-based restriction enforcement), active mediation (dialog about media, both instructive and critical), and co-use (modeling and shared media experience). Though technical mediation is sometimes defined as a subset of active mediation and not restrictive mediation (Sevilla-Fernández et al., 2025), this paper considers technical mediation the subset of active mediation and restrictive mediation that can be achieved through technical means. Since co-use is always an interactive mediation method, it cannot be achieved

solely through technical means and is excluded. By this overall definition, features identified in the literature encompass the entire space of technical mediation.

Technical mediation is similar to parental controls but not synonymous. Technical mediation is the automated ability to accomplish parental mediation. Parental controls are features within a parental control system whose primary purpose is to enforce technical mediation through predefined policies. Even though parental control systems are the primary application of this research, special purpose software that needs to implement technical mediation features could leverage these findings as well. An example would be a video game system complying with applicable laws but not needing to integrate a fully featured parental control system.

**Features & Controls Identified**

Features discussed in academic literature were often described in a general manner and could not be directly used as a technical requirement without further interpretation or creativity. Twenty three specific features were described, all fitting into eight feature categories and described below. Depending on the structure and purpose of the study, each article described a feature in either a restrictive manner (typical for restrictive mediation) or a monitoring manner (typical for active mediation but sometimes leveraged for manual restrictive mediation). From a technical perspective all features that can be monitored can also be restricted, and vice versa. For this reason, even if a feature was only described as monitored or only described as restricted, its alternative was also included as a feature to target.

Finally, some features fit into multiple categories and describe dynamic controls (monitoring and restricting that informed and directed each other). These features require logic and a workflow definition. However, since they still fall under the realm of technical mediation, they are included independently as logic features.

### *Time-based Features*

The features most often described in the literature were time-based. This was sometimes simply described as screen time or social network time (Rudnova et al., 2023). If the amount of time a device, application, or site was monitored or restricted then the impact of screen time on a child could be controlled, discussed, or considered as part of parental mediation. This correlates to the highest concern among caregivers: screen addiction (Ziker et al., 2025). This is notable because regulating “the screen” (or, more accurately, overall device usage) is the broadest control possible. Other features delve into varying levels of granularity: by application, website category, specific website, usage location correlated to application usage, etc. However, regulating device usage based on a time constraint only requires two states (accessible or inaccessible). This may be tied to caregivers’ concerns that screen time competes with children’s physical activities and real-world social interactions as a whole (Aslan et al., 2024). A binary control based on time can accomplish this goal.

The need to regulate screen time was primarily described as a time limit to the entire device or to a specific application (Sevilla-Fernández et al., 2025), e.g. permitting one hour of social network app use. When caregivers described in detail their current practices of mediation (Kotrla Topić et al., 2023) or perception of harmful use (Lukavská & Gabrhelík, 2024) they also described limiting the time of day, e.g. not permitting device access after bedtime. This loosely aligned with guidance provided by the American Academy of Pediatrics (2024) when advising caregivers to consider if media use while falling asleep is a negative coping mechanism.

Kotrla Topić et al. (2023) also recorded caregivers had different time restrictions based on the day of the week, e.g. an additional hour of usage is permitted on the weekend. Scheduled usage by time of day and scheduled usage by day of week were identified as two separate features even though they are related. Scheduled usage by day of week could be considered a variation of scheduled usage by time of day with additional logic (and therefore included in the Logic category of features). However, defining a schedule for usage is the basis

for the feature and not a ruleset in addition to the single-day schedule feature. Defining a schedule for a day can be done with minimal timekeeping or internationalization concepts. Defining a schedule beyond a daily recurrence (e.g. recurring by week, month, or fully customized) requires more awareness of calendar systems and internationalization. The features were separated due to this additional complexity.

Monitoring and reporting on screen time was also described. Screen time monitoring directly enables active mediation, and allows adherence to the Teen Online Safety Strategies (TOSS) framework (Wisniewski et al., 2017). Monitoring is also an important component in a distant mediation strategy, and it may be needed in a laissez-faire parenting style (Livingstone et al., 2017).

While outside the realm of mediation, Kotrla Topić et al. (2023) found that caregivers reported screen time restrictions as a punishment and additional screen time as a motivation. A parental control system should enable caregivers to perform this action, and presuming the screen time restriction is temporary this feature would be time-based (e.g. device is inaccessible for 3 hours). The four time-based features identified are listed in Table A1.

### *Content-based Features*

Following time-based features, content-based features were the second most common type of feature described by caregivers and researchers. Basic content filtering was rarely mentioned by itself in recent literature. This may reflect the conclusions of historical research on content restrictions (see Livingstone & Helsper, 2008) and the direction of modern research in exploring new topics. Current surveys, however, reveal that content restriction and monitoring is still on caregivers' minds. Kotrla Topić et al. (2023) found some caregivers restrict specific apps completely (e.g. Instagram is not allowed). Ziker et al. (2025) confirmed the existing precedent that caregivers are interested in website content filtering (in addition to mobile app filtering) and concluded that content filtering capabilities continue to evolve. Ziker et al. specifically report that one of the most common controls used are child profiles (e.g. YouTube Kids) due to their ease

of setup. Child profiles and other curated content services are a form of content restriction that lack granularity and require the vendor to maintain.

While some caregivers in the study included malware protection as a form of parental control (Ziker et al., 2025), this is different from a parental control since it is commonly a self-protection action taken and not isolated to parental mediation. It was therefore not considered a parental control feature.

Specialized studies focused on content exposure online among youth. This included research into game addiction by Kapetanovic et al. (2025) that required monitoring of specific categories of applications and websites. Dynamic content was studied by Punnaivanam and Velvizhy (2024) in an effort to filter AI generated text, though this need can be extended to other AI generated content like pictures and videos, and to user generated content that is difficult to identify by URL. Dynamic content extends to apps and their analysis as Hakami (2025) described while dynamically permitting applications. Granularity is important, though, as demonstrated by Anderson et al. (2024) in their comparison of damaging types of sexual violence media with informative types of sexual violence media.

Content is one of the “5 C’s” described by the American Academy of Pediatrics (2024). Allowing caregivers to consider media content for their children would require all the above mentioned features (monitoring apps, websites, and website categories, as well as restricting all three). The AAP is not the only study to emphasize monitoring over restriction – it is a common technique to support active mediation and restriction negotiation (Kotrla Topić et al., 2023). The four content-based features identified are listed in Table A1.

### *Contact-based Features*

Two series of features were specific to online social interaction and nuanced enough to be considered apart from content-based features and described in their own categories. The first was managing contacts. Sevilla-Fernández et al. (2025) identified contacts as a main risk in social networks. In their survey of caregivers’ existing use of parental controls, Ziker et al.

(2025) found one of the primary ways caregivers manage risks associated with external media influences is by defining rules and limits around interacting with strangers online.

Restricting or monitoring contacts may be achievable through content-based features (i.e. if the contact is part of the filterable content). For better accuracy and privacy, however, it should be considered separate. In content-based controls, content is evaluated while access to the device or browser is generally unrestricted. In contact-based controls, access to the communication medium is restricted by who communication occurs with (i.e. the contact), while the content of the communication is unregulated. This distinction was the basis of Ghosh et al.'s (2020) study to introduce teen privacy into parental controls.

Contact management was also identified in conjunction with content management. In a study of media and sexual violence, sexting was associated with harmful attitudes and behaviors (Anderson et al., 2024). Caregivers can address sexting through a combination of managing what is downloaded (content-based features), who is contacted (contact-based features), and what is uploaded (sharing-based features, described below). The three contact-based features identified are listed in Table A1.

***Sharing-based Features***

The other feature related to online social interaction was sharing-related features. In addition to the content consumed by children, caregivers are interested in restricting and even approving the content that is produced and uploaded to social media (Kotrla Topić et al., 2023). This may be included in concerns and restrictions described as "privacy" (Ziker et al., 2025) though that category also includes financial vulnerability and exposure to scams. Sharing was described as a feature needing granular control since the motivation can be generic based on moderation goals (Kotrla Topić et al., 2023) or specific based on content (Anderson et al., 2024). Anderson et al. also described Technology Facilitated Sexual Violence which can be enabled by media sharing. If parental control technology can notify, request approval, or restrict-

and-notify when content upload rules are triggered caregivers would be able to utilize those controls for active mediation as well.

Interactive or real-time social media interactions can also pose a risk. Cyberagression was identified as a common topic of research by Sevilla-Fernández et al. (2025). Since cyberaggression and bullying is a complex topic requiring informed and coordinated active mediation (Sadiku, 2024), content- and context-aware sharing controls would be required to address its unique risk. The two sharing-based features identified are listed in Table A1.

### *Physical and Device Features*

Some features described by caregivers depend on physical characteristics. This was often described as enabling or restricting smartphone usage during an activity defined by its location, like during family mealtime or school (Kotrla Topić et al., 2023). Technical limitations in location processing create a natural boundary between coarse and fine location resolution. The physical location feature was subdivided into a macrolocation feature (when coarse granularity of location is required) and a microlocation feature (when fine granularity of location is required). Both are on caregivers' minds: in their study of relational and personal activities, Lukavská and Gabrhelík (2024) identified 14 activities incompatible with smartphone usage in the opinion of caregivers, the majority of which were defined by real-world location. Macrolocation activities like attending cultural events can be defined by a general location like museum or performance venue. Microlocation activities like family mealtimes can be defined by a specific location like the dining room area in the house (but not the living room or bedroom).

Family mealtime usage was the most common location-based feature. Martins et al. (Martins et al., 2020) found a strong correlation between internet addiction and internet usage during family mealtime. This underscores the need to provide location-based features in parental controls. It is worth noting that even though Martins et al. identified addiction correlations between both adolescents' and caregivers' internet usage, addressing caregivers' internet usage is out of the scope of this paper.

Another physical characteristic related to device usage centered on physical activity performed by the child. Kotrla Topić et al. (2023) describes caregivers' concerns around using technology during time spent outside or time playing. While this could be addressed through location-based restrictions it can also be predicted by biometrics like elevated heart rate. Caregivers dislike device usage while walking or hiking together (Lukavská & Gabrhelík, 2024). The impact of digital media on young children's needs for physical activity has also been studied (Aslan et al., 2024) though this may be a challenging target for biometric based restrictions. The detected scenario must be compatible with measurable biometric sensors: exercising while listening to music on a smartphone may be achievable; playing games on a smartphone instead of exercising would be perceived as no elevated biometric data. Biometric information may be limited in parental control situations.

The American Academy of Pediatrics (2024) encourages caregivers and clinicians to consider what activities are being crowded out by increased media usage and screen time. Physical activities (like time outdoors) and location-based activities (like quality family time) are given as examples, further supporting the need to provide "in real life" monitoring and restricting capabilities in parental controls. The three physical and device features identified are listed in Table A1.

### *Monetary Features*

A few articles described purchase and money related restrictions. This was generic, typically described as "online purchases" (Ziker et al., 2025). That can have a range of implications, from restricting online purchase of goods (e.g. making an unapproved Amazon order) to payment of services (e.g. paying an undisclosed medical bill) to the purchase of software (e.g. subscribing to a video game service). However, the purchase of online apps and in-app purchases may be the actual need imagined by caregivers since, when it is specified, restrictions to purchasing apps (Sharma & Lee, 2024) or in-app purchases (Wardle & Zendle, 2021) are the only scenarios described.

Though not directly listed by caregivers, a monetary risk discussed by researchers was gambling as it relates to internet addiction (Sevilla-Fernández et al., 2025). Riley et al. (2021) documents that up to 89.9% of youth have been exposed to gambling, and that experience with online gambling during adolescence increases the risk for problem gambling. Since some online transactions like in-app purchases have been observed to share characteristics with online gambling and problem gambling (Wardle & Zendle, 2021) the ability to control monetary transactions based on youth gambling risk is a valid feature of a parental control system. The two monetary features identified are listed in Table A1.

### *Connectivity Features*

Even more rarely mentioned than monetary features were that of broad connectivity management. Ziker et al. (2025) observed that some caregivers monitor phone calls and text messages. They concluded this may simply be an analog method of control used by less digitally fluent caregivers. Monitoring phone calls was taken to mean a call log and not a transcript or recording of the call. Monitoring text messages was already identified as feature N3 and not included in the Connectivity category. In their survey of parental control applications, Wisniewski et al. (2017) found less than a third of applications supported call monitoring, call blocking, and text message blocking (25%, 28%, and 21%, respectively). They also found a small number of parental control applications supported restricting data connections like Wi-Fi and Bluetooth, though a need for these restrictions was not reported by caregivers or researchers. The single connectivity feature, manage telephone calls, is listed in Table A1.

### *Logic-based Features*

Finally, some features described required multiple domains of information or the collaboration of more than one feature. The most basic logic feature was a combination of time and content management, as Kotrla Topić et al. (2023) described a caregiver might limit the amount of time allowed on a specific app or website. This would also be needed to address the tension between education-benefiting usage and education-harming usage while still permitting

wider access outside of school and study periods. Other features required interpretation: Ziker et al. (2025) noted that “wasting time” was one of youth’s top self-reported risks of technology platforms. To identify and then monitor or restrict wasting time a parental control system would need to be aware of content and context (e.g. using a social media app at a school location; texting peer contacts during study hours; etc.) depending on how wasting time is defined.

Other features were more nuanced. Though most studies focused on a narrow range of ages, Wang et al. (2023) concluded that caregivers desired and implemented different restrictions based on the child’s age. Children age and mature while remaining subject to parental controls and technical mediation. This requires a dynamic and age-based rule management feature of a parental control system.

Another feature was transparency. Kapetanovic et al. (2025) found a correlation between internet gaming disorder and youth secrecy towards their caregivers. Stoilova et al. (2024) described the tendency of children to circumvent parental controls. Considering both features together a parental control system may need to identify behavior patterns and activity anomalies. The four logic-based features identified are listed in Table A2.

**Summary of Literature Review**

Parental mediation and technological controls supporting mediation is an established field of study and as such many desired features are identified in academic literature. Features were organized into eight categories based on the type of action they took or the input they needed to function. These eight categories included seven basic monitor-restrict features (time-based, content-based, contact-based, sharing-based, physical & device, monetary, and connectivity) and one cross-domain category called logic-based features. All 23 features are listed in Appendix A: Table A1 lists the 19 basic features by category and Table A2 lists the four logic-based features.

## Findings

By mapping the 23 features to NIST's Cybersecurity Framework we can create a cybersecurity-aware specification of a parental control system that meets all the needs described by caregivers and researchers. As a visual reference the entire mapping process is described for a single feature in Appendix B, Feature Mapping Example. CSF functions are described below in the order they were derived from the literature (protect, respond, identify, detect). A complete list of findings is presented in Appendix C, Catalog of Findings, in the traditional CSF order (identify, protect, detect, respond).

### Initial Direct Mapping

Even though the literature reviewed discussed all the needs and outcomes of parental and technical mediation, parental control features were most often described in language aligning to CSF's Protect or Respond functions. An example of this derivation is shown in the top half of Appendix B, mapping paraphrased findings from the literature to monitoring and restricting capabilities. Features in modern literature align to desired actions rather than unaddressed risks. This is understandable considering the application of technology to parental mediation is nearly 20 years old and mature. Thierer's (2009) survey of parental control tools and methods devotes a section to identifying risks and defining rationale. Risks have since become less articulated and only actions to be taken are described. In their study on motivations behind parental mediation, Sharma and Lee (2024) started with the observation that caregivers can restrict purchases, content, and schedules of a child's media usage, then worked backward to understand associated parental style. They did not, however, describe the risks the caregivers hoped to avoid through parental controls.

As we are describing a technical parental control system and not the entire spectrum of parental mediation the parental style is irrelevant and the function of the system is presumed. The risk being addressed by the parental control system must be identified. When only Protect or Respond actions were described, the risk (aligning to the CSF Identify function) had to be

extrapolated. This is important to ensure that a control, when implemented, can be evaluated as sufficient or insufficient.

### *Protect Function*

The need to monitor technology was described independent of a caregiver's need to restrict technology. This facilitates active mediation, parental style, and the changing needs of children as they grow. Monitoring capabilities mapped to CSF's Protect function. Most outcomes were described as accessing the sensor and reporting on it, such as N1.PR (access text messages, report on recipients). For some outcomes, the sensor information is not presumed to exist, requiring both collection and reporting (as in C2.PR, record app/website consumption, report by each endpoint). One feature was restrictive only and did not have a Protect outcome: feature T4 (temporary access) is driven by the caregiver's situational awareness (e.g. change in circumstances, punishment, etc.) and a Protect outcome does not apply. All Protect outcomes are listed in Appendix C with the suffix PR.

### *Respond Function*

The need to prevent youth activities mapped to CSF's Respond function. This facilitates restrictive mediation which is the most frequent feature associated with parental controls (Ionescu, 2023). Restrictive mediation, and the ability to respond to perceived online threats, is effective in achieving certain goals. Sevilla-Fernández et al. (2025) found that restrictive mediation was faster and more effective than active mediation in controlling and reducing usage time and frequency (specifically among social network usage). A modern parental control system cannot be reduced to restrictions alone, however, as emphasized by the Teen Online Safety Strategy framework (Wisniewski et al., 2017) which explicitly aims to balance active mediation with restrictive mediation and parental control with child self-regulation. This reiterates the need to view a parental control's Respond function (supporting restrictive mediation) in cooperation with its Protect function (supporting active mediation).

Most outcomes blocked content or prevented action, the exceptions being P1 (manage telephone calls) and S2 (approve social media activity). Managing telephone calls was never described in the literature as a restrictive feature (i.e. I cannot prevent my child from making or receiving a phone call) so its Respond function was not included. Approving social media activity may contain a blocking component, e.g. the AI engine detects the sharing of nude images which violates the parental control policy (discussed in the Detect function below) and automatically blocks the sharing action. (S1, manage social media activity, targets the action as a whole, e.g. preventing liking, friending, or sharing generally.) Approving social media activity may also defer the sharing action depending on the policy, e.g. the AI engine detects the sharing of uncensored faces, encounters a policy requiring approval of sharing personally identifiable images, and pushes an approval request to the caregiver. This real-time response is similar to the Pause Reflect Redirect Level 3 intervention (Sweigart et al., 2025).

All Respond outcomes would automatically continue normal operation once the restricted action ceased. Time-based functions would restore capabilities once the time limit or triggered schedule had passed. Content-based functions would restore operation once an unrestricted site or application was loaded. Physical and Device functions would work after the device was moved to an unrestricted location, or biometric data returned to unrestricted levels. All Respond outcomes are listed in the Catalog of Findings appendix with the RS suffix.

**Identify Function**

After parental control features define a Protect or Respond outcome, the corresponding Identify outcome can be quantified. Identify outcomes indicate a risk and as previously stated all parental control features address a risk though they are not always explicitly described in current literature. The risk is phrased as a technical limitation by a caregiver, as in C1.ID (I do not know or cannot control what types of sites my child sees on app/website). Since we are only describing a technical system, an Identify outcome does not describe the reasoning behind a caregiver's stated risk or the consequences of that risk. Those details are defined by the specific

parental control instance and the caregiver putting the system in place to achieve their goals and convey their family values.

Risks identified in the logic category closely followed shortcomings mentioned in literature and required less interpretation. Wang et al. (2023) found that restrictive mediation decreased as children age. Therefore, a limitation to be addressed in a parental control system would be to automatically adjust rules based on the child's age (L1.ID). Kapetanovic et al. (2025) found that secrecy around internet use was a predictor of internet gaming disorder, which can be directly rephrased as the risk L2.ID (I do not know when my child is trying to hide online activity, and cannot change rules appropriately). Only risk L4.ID (restrictions are not smart enough) was indirectly derived as it represented a composite feature described in the literature through example, e.g. restrictions “frequently involve both time and content” (Kotrla Topić et al., 2023, p. 212). The Catalog of Findings appendix lists all Identify outcomes using the suffix ID.

**Detect Function**

All restrictions were conditional apart from blocking temporary access (T4). Conditional Respond outcomes implied a subset of activity that must be detected and this activity was derived to determine the feature’s Detect outcome. This required defining specific criteria to detect, as in S1.DE (blacklist of sharing action/behavior is detected). In this case, the Respond outcome is the prevention of the detected action, as in S1.RS (prevent blacklisted sharing action/behavior). For the Time category, detection criterion is best described as a schedule (e.g. T2.DE, usage occurs outside of daily schedule). A convention of explicit activities is used to describe outcomes for simplicity, i.e. a whitelist of permitted activities or a blacklist of restricted activities. Implementation of parental controls can use either a blacklist or whitelist for monitoring or restricting to achieve best usability.

Feature T4 (temporary access) was described in the literature as a capability of a parental control system and not as a risk of digital media. It was often described in the form of

enforcing restrictions or enacting punishment (Kotrla Topić et al., 2023). When blocking access for the purpose of punishment, the risk (Identify), context (Prevent), and initiation (Detect) of the blocking is not technical and is based on the caregiver's judgement. The capability was still included as a feature of a parental control system since it is similar to actions taken during the containment phase of incident response (SANS Institute, n.d.) and as such is a cybersecurity function. All Detect outcomes are listed in Appendix C with the suffix DE.

**Lack of Recover Function**

No technical controls fit into CSF's definition of the Recover function, defined as actions that support "the timely restoration of normal operations" (National Institute of Standards and Technology, 2024, p. 4). The CSF was designed to reduce cybersecurity risk among information and communications technologies (ICT). In defining parental control features using CSF we are addressing risk not just in ICTs such as laptops and mobile phones but also in youth by modeling them as an ICT system subject to parental controls following CSF's Govern function. Modeling a human as a technology system has obvious shortcomings, one being recovery. The mental, physical, and emotional recovery of a child was not described through technical means in the literature reviewed. Sweigart et al. (2025) describes a method to achieve a human-centered Recover function in very specific scenarios but the method was not easily transferable to all parental control features.

Consider as an example the download of an image from an unapproved website that should be blocked (i.e. feature C2 in Appendix A). The parental control system maintains the policy concerning the approved and unapproved websites (Govern). The policy was defined by the caregiver based on the specific needs of the child and goals of the caregiver (Identify). Traffic on the youth's device is monitored and evaluated against the policy (Protect). When the traffic violates the policy (Detect) the traffic is not delivered to the youth's device (Respond). The technical system – the youth's computing device – is not itself compromised and can function normally by navigating to an approved site. The device does not need recovery. Should the

Respond outcome delay to activate or fail completely the unapproved content is a threat to the mental, physical, and/or emotional wellbeing of the child. It is not a threat to or impede the functionality of the computing device.

Malware prevention is a concern some caregivers note in the literature. While malware prevention contains a recovery component that targets a technical system, malware prevention is a general concern and not specific to parental control systems. It was considered out of scope for parental control feature analysis.

If the Respond outcome succeeds and the unapproved content is blocked, the continuous browsing experience of the youth has been broken. The explanation of the policy violation and steps to prevent future violation is a part of active mediation and caregivers practice it through discussion and co-use (Kotrla Topić et al., 2023). Many existing applications fulfill this need through a seek-help or “SOS” feature allowing a youth-initiated, context-aware notification to be delivered to a caregiver (Wisniewski et al., 2017). A context-aware description of the policy applied and action taken can also be implemented in a parental control system, further facilitating active mediation (Sweigart et al., 2025). However, these are all implementation details of a parental control system intended to support parent-child interaction and not technical controls. As such they have been excluded from CSF mapping to provide implementation flexibility. The technical basis for such features is supplied by the feature’s Identify outcome (reporting, monitoring, transparency, etc.) and no additional capabilities are needed.

### Feature-Specific Considerations

As features were identified in literature some included specific details that would impact how a parental control system should address them.

#### *Macrolocation and Microlocation*

Literature often described mediation requirements based on activities best defined by a location. Lukavská and Gabrhelík (2024) noted multiple location-based activities that caregivers

considered smartphone usage detracting to, including family mealtimes and while attending cultural events like a concert. Modern smartphones contain GPS receivers to aid with location features like driving directions. Such receivers are accurate to within 16 ft (National Coordination Office for Space-Based Positioning, Navigation, and Timing, 2022). While parental control systems protect all internet-connected devices accessible by children, smartphones are one of the most popular devices children use to access the internet (Act for Youth, 2024). As such GPS-capable features are most likely readily available for location-sensitive features. Location restrictions that can be defined within the 16 ft accuracy of a smartphone GPS receiver were categorized as macrolocation restrictions. Examples of macrolocation include the entirety of a child's school grounds, an entire theater building, and a restaurant. By using GPS-based geofencing rules macrolocation restrictions can be achieved with no additional hardware beyond a smartphone.

Other locations required either a location accuracy finer than 16 ft or a location relative to another person. These locations were categorized as microlocation. Examples of microlocation include a dining room (targeting family mealtime) or a caregiver's smartwatch (targeting interaction with that caregiver). Accuracy finer than smartphone GPS receivers is achievable through Bluetooth Low Energy triangulation and accurate up to 4 in. based on beacon placement (Park et al., 2016). Relative locations can also utilize Bluetooth signal strength to determine proximity but can only detect a Bluetooth-enabled device and not a person per se. Since microlocation restrictions represent a distinct but achievable feature from macrolocation they are described separately. Achieving microlocation restrictions may require more configuration than macrolocation restrictions in the form of stationary beacons or additional caregiver software.

### *Technical Limitations as Boundaries*

Outcomes related to specific technical limitations were isolated to improve implementation. This was done with the separation of contact management between text

messaging contacts (N1) and social media contacts (N2). Depending on how social media contacts are defined and managed, integrations may need to be specific to each social media platform (e.g. the management of TikTok contacts requires an integration unique from the management of Telegram contacts). Regardless of how it is managed, social media contacts will be managed in the OSI Application layer through API calls. In this manner all social media contact management can be described together.

Text messages that are sent over SMS or MMS protocols are not sent over the internet. Monitoring or restricting text message contacts requires a different approach from social media contact management. The only user-controlled device an SMS/MMS message routes through is the sending or receiving device; the mobile switching, short message service center, and signal transfer points (Osho et al., 2014) are similar to an internet service provider and are not available to a caregiver to apply parental controls. Since the technology to apply parental controls differs drastically between SMS/MMS and internet-based applications these outcomes were separated. N1 concerns text messaging contacts while N2 concerns social media contacts. N3 is specific to text messaging content. Review, approval, and restriction of social media content is a subset of internet content and is addressed through other controls: C2 can be used to manage specific social media platforms, C3 can manage downloaded dynamic content, S1 can manage social media activities, and S2 can be used to manage uploaded content.

## Recommendations

Academic literature is aware of parental control needs and describes accurately the features caregivers and researchers are interested in. All features can be mapped onto Cybersecurity Framework 2.0 functions as unique outcomes. Each outcome can be leveraged to develop new parental control systems or evaluate existing systems. When implementing a new parental control system a developer should ensure all applicable features listed in Appendix A are in scope and delivered. The granularity listed in Table A1 is derived from the

literature based on the context of the feature described, although it may not be feasible (too generic) or complete (too specific) depending on how the system is implemented. (Granularity listed in Table A2 is specific to each feature.) If a developer needs clarification on the goal or function of a feature they can consult the CSF mapping in Appendix C. By addressing the need listed in the Identify outcome, or implementing controls to address Protect, Detect, and Respond outcomes, the system developer can ensure they have accurately implemented the feature. If a researcher advocates a novel feature for parent control they can use Appendix B, Feature Mapping Example, as a guide to map the feature onto cybersecurity-aware outcomes in the CSF 2.0 framework.

For example, while the manage content by category feature (C1) is being developed, a systems architect can design around the specific risk being addressed, C1.ID (I do not know or cannot control what types of sites my child sees on app/website). According to the Protect outcome C1.PR endpoint categorization is necessary. This implies an intelligence feed of existing and future websites and API endpoints must (a) be maintained, (b) include website & endpoint categorizations, and (c) be available to the parental control system. This could require a client-server architecture, or the parental control developer may achieve this through another method.

Existing parental control systems can be audited using the Catalog of Features (Appendix C). For example, a systems analyst uses the catalog to identify gaps in features and identifies the system can detect social media likes and share (S1.DE) but cannot prevent sharing (S1.RS). The developer originally addressed the concern by preventing all access to the social media platform but the catalog feature S2 (approve social media activity) is more granular than the implemented feature. The analyst has identified a missed feature that caregivers and researchers desire. Auditing can be extended to non-parental control systems that require the addition of a subset of controls. For example, an internet-capable video game console engineer

can select technical mediation features relevant to the internet experience they are providing to integrate useful mediation controls.

Additional research can contribute to the topic. Features identified in literature were generic and lacked technical specificity. Caregivers can be interviewed on what specific, technical features are needed from a parental control system. Existing systems can be reviewed to understand specific controls already in place and their degree of use. Some features are easier to implement than others on current computing devices: preventing access from a desktop browser to a website is easily achievable through a traditional firewall. Preventing access to a specific API call from a proprietary mobile app to a closed source API endpoint may be achieved through proxy configuration and trusted certificates. However, the walled garden nature of mobile operating systems and consumer applications may present other challenges to traditional networking methods and deep inspection. Research can be performed to identify and address implementation challenges in modern devices. Where necessary, policy changes can be proposed to compel device and application developers to provide the integrations required to give caregivers control over their children’s internet experience to better raise the next generation to have a healthy and balanced relationship with technology.

**References**

Act for Youth. (2024, April 17). *Youth statistics: Internet and social media*. https://actforyouth.org/adolescence/demographics/internet.cfm

Akter, M., Godfrey, A. J., Kropczynski, J., Lipford, H. R., & Wisniewski, P. J. (2022). From Parental Control to Joint Family Oversight: Can Parents and Teens Manage Mobile Online Safety and Privacy as Equals? *Proc. ACM Hum.-Comput. Interact.*, *6*(CSCW1). https://doi.org/10.1145/3512904

American Academy of Pediatrics. (2024, April 6). *How to use the 5 Cs of media use: Tips for pediatric clinicians*. https://www.aap.org/en/patient-care/media-and-children/center-of-excellence-on-social-media-and-youth-mental-health/how-to-use-the-5-cs-of-media-use-tips-for-pediatric-clinicians/

Anderson, K. M., Macler, A., Bergenfeld, I., Trang, Q. T., & Yount, K. M. (2024). The Media and Sexual Violence Among Adolescents: Findings from a Qualitative Study of Educators Across Vietnam. *Archives of Sexual Behavior*, *53*(6), 2319–2335. https://doi.org/10.1007/s10508-024-02869-7

Aslan, S., Durham, L. M., Alyuz, N., Chierichetti, R., Denman, P. A., Okur, E., Aguirre, D. I. G., Esquivel, J. C. Z., Cordourier Maruri, H. A., Sharma, S., Raffa, G., Mayer, R. E., & Nachman, L. (2024). What Is the Impact of a Multi-Modal Pedagogical Conversational AI System on Parents' Concerns About Technology Use by Young Children? *British Journal of Educational Technology*, *55*(4), 1625–1650. https://doi.org/10.1111/bjet.13399

Assie, M. (2024, May 27). *How AOL changed the way we use the internet: A retrospective*. Medium. https://medium.com/@mail_18109/how-aol-changed-the-way-we-use-the-internet-a-retrospective-e067c1822cbd

Burch, K. (2025, March 19). *My tweens found a way around the parental controls on their devices. Google paid them thousands to explain how.* Business Insider.

https://www.businessinsider.com/tweens-found-way-around-the-parental-controls-on-their-devices-2025-3

Burgess, J. (2025, January 31). Giving my kid an iPhone is scary. Here's why I'm glad I did. *USA TODAY (USA)*, A7.

Center for Internet Security, Inc. (2021, May). *CIS controls version 8*. https://www.cisecurity.org/cis-benchmarks

Chandramouli, R. (2022). *Guide to a secure enterprise network landscape*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-215

Chen, V. H. H., & Chng, G. S. (2016). Active and Restrictive Parental Mediation Over Time: Effects on Youths' Self-Regulatory Competencies and Impulsivity. *Computers & Education*, *98*, 206–212. https://doi.org/10.1016/j.compedu.2016.03.012

Duchaussoy, Q. (2020). *Security and Privacy Analysis of Parental Control Solutions* (public; p. 85) [Concordia University]. https://spectrum.library.concordia.ca/id/eprint/987584/

Elmogy, A., & Elkhowiter, K. (2017). Parental Control System for Mobile Devices. *International Journal of Computer Applications*, *177*(3), 16–23. https://doi.org/10.5120/ijca2017915687

Ghosh, A. K., Hughes, C. E., & Wisniewski, P. J. (2020). Circle of Trust: A New Approach to Mobile Online Safety for Families. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–14. https://doi.org/10.1145/3313831.3376747

Haidt, J. (2024). *The anxious generation: How the great rewiring of childhood is causing an epidemic of mental illness*. Penguin Press.

Hakami, H. (2025). Automatic Classification of Mobile Apps to Ensure Safe Usage for Adolescents. *PLoS One*, *20*(1). https://doi.org/10.1371/journal.pone.0313953

Ionescu, S. (2023, June 22). *What are parental controls and do they work?* TechRadar. https://www.techradar.com/features/what-are-parental-controls-and-do-they-work

Joint Task Force Interagency Working Group. (2020). *Security and privacy controls for information systems and organizations* (Revision 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Kapetanovic, S., Maiken Due Nielsen, André, F., Gurdal, S., & Claesdotter-Knutsson, E. (2025). Exploring Parent-Child Relationships in a Swedish Child and Adolescent Psychiatry—Cohort of Adolescents with Internet Gaming Disorder. *BMC Psychology*, *13*, 1–10. https://doi.org/10.1186/s40359-024-02306-3

Kirkland, D. (2025, January 6). *A proud dad's tale of two bug hunting daughters*. https://blog.dustinkirkland.com/2025/01/a-proud-dads-tale-of-two-bug-hunting.html

Kotrla Topić, M., Perić Pavišić, K., & Merkaš, M. (2023). A Qualitative Analysis of Parental Mediation of Children's Digital Technology Use in Croatia. *Journal of Broadcasting & Electronic Media*, *67*(2), 206–224. https://doi.org/10.1080/08838151.2023.2182786

Livingstone, S., & Helsper, E. J. (2008). Parental Mediation of Children's Internet Use. *Journal of Broadcasting & Electronic Media*, *52*(4), 581–599. https://doi.org/10.1080/08838150802437396

Livingstone, S., Ólafsson, K., Helsper, E. J., Lupiáñez-Villanueva, F., Veltri, G. A., & Folkvord, F. (2017). Maximizing Opportunities and Minimizing Risks for Children Online: The Role of Digital Skills in Emerging Strategies of Parental Mediation. *Journal of Communication*, *67*(1), 82–105. https://doi.org/10.1111/jcom.12277

Lukavská, K., & Gabrhelík, R. (2024). Parental Views on Their Children's Smartphone Use During Personal and Relational Activities. *PLoS One*, *19*(8). https://doi.org/10.1371/journal.pone.0308258

Martins, M. V., Formiga, A., Santos, C., Sousa, D., Resende, C., Ricardo Campos, Natália Nogueira, Paula Carvalho, & Sofia Ferreira. (2020). Adolescent Internet Addiction—Role of Parental Control and Adolescent Behaviours. *International Journal of Pediatrics and Adolescent Medicine*, *7*(3), 116–120. https://doi.org/10.1016/j.ijpam.2019.12.003

National Coordination Office for Space-Based Positioning, Navigation, and Timing. (2022, March 3). *GPS accuracy*. https://www.gps.gov/systems/gps/performance/accuracy/

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

Osho, O., Ogunleke, O. Y., & Falaye, A. A. (2014). Frameworks for Mitigating Identity Theft and Spamming Through Bulk Messaging. *2014 IEEE 6th International Conference on Adaptive Science & Technology (ICAST)*, 1–6. https://doi.org/10.1109/ICASTECH.2014.7068119

Park, H., Noh, J., & Cho, S. (2016). Three-Dimensional Positioning System Using Bluetooth Low-Energy Beacons. *International Journal of Distributed Sensor Networks*, *12*(10), 1550147716671720. https://doi.org/10.1177/1550147716671720

Punnaivanam, M., & Velvizhy, P. (2024). Contextual Fine-Tuning of Language Models with Classifier-Driven Content Moderation for Text Generation. *Entropy*, *26*(12), 1114. https://doi.org/10.3390/e26121114

Riley, B. J., Oster, C., Rahamathulla, M., & Lawn, S. (2021). Attitudes, Risk Factors, and Behaviours of Gambling Among Adolescents and Young People: A Literature Review and Gap Analysis. *International Journal of Environmental Research and Public Health*, *18*(3), 984. https://doi.org/10.3390/ijerph18030984

Rudnova, N., Kornienko, D., Semenov, Y., & Egorov, V. (2023). Characteristics of Parental Digital Mediation: Predictors, Strategies, and Differences Among Children Experiencing Various Parental Mediation Strategies. *Education Sciences*, *13*(1), 57. https://doi.org/10.3390/educsci13010057

Sadiku, A. (2024). Positive and Negative Impacts of Technology Use in Young Children: The Need for Parents to Learn How to Guide Their Children in Using Technologies. *Croatian Journal of Education / Hrvatski Časopis za Odgoj i Obrazovanje*, *26*(3), 1001–1027. https://doi.org/10.15516/cje.v26i3.5488

SANS Institute. (n.d.). *Incident response*. Retrieved June 27, 2025, from https://www.sans.org/security-resources/glossary-of-terms/incident-response/

Sevilla-Fernández, D., Díaz-López, A., Caba-Machado, V., Machimbarrena, J. M., Ortega-Barón, J., & González-Cabrera, J. (2025). Parental Mediation and the Use of Social Networks: A Systematic Review. *PLoS One*, *20*(2). https://doi.org/10.1371/journal.pone.0312011

Sharma, S., & Lee, C. Y. (2024). Parental Mediation and Preferences for Regulation Regarding Children's Digital Media Use: Role of Protection Motivation and Theory of Planned Behaviour. *Behaviour & Information Technology*, *43*(8), 1499–1517. https://doi.org/10.1080/0144929X.2023.2217275

Skiera, A. (2024, September 10). *What Gen Z thinks about its social media and smartphone usage*. Harris Poll. https://theharrispoll.com/briefs/gen-z-social-media-smart-phones/

Stoilova, M., Bulger, M., & Livingstone, S. (2024). Do Parental Control Tools Fulfil Family Expectations for Child Protection? A Rapid Evidence Review of the Contexts and Outcomes of Use. *Journal of Children and Media*, *18*(1), 29–49. https://doi.org/10.1080/17482798.2023.2265512

Stouffer, C. (2022, September 29). *How to set parental controls on every device: An absolutely ultimate guide*. https://us.norton.com/blog/how-to/how-to-set-parental-controls

Sweigart, E. A., Valliani Aahil, & Wisniewski, P. J. (2025). Pause, Reflect, and Redirect: An Approach to Empowering Youth to Be Safer Online by Helping Them Make Better Decisions. *Social Sciences*, *14*(5), 302. https://doi.org/10.3390/socsci14050302

Thierer, A. D. (2009). *Parental controls & online child protection: A survey of tools & methods*. https://doi.org/10.2139/ssrn.1268433

Wang, M., Lwin, M. O., Cayabyab, Y. M. T. M., Hou, G., & You, Z. (2023). A Meta-Analysis of Factors Predicting Parental Mediation of Children's Media Use Based on Studies

Published Between 1992–2019. *Journal of Child & Family Studies*, *32*(5), 1249–1260. https://doi.org/10.1007/s10826-022-02459-y

Wardle, H., & Zendle, D. (2021). Loot Boxes, Gambling, and Problem Gambling Among Young People: Results from a Cross-Sectional Online Survey. *Cyberpsychology, Behavior, and Social Networking*, *24*(4), 267–274. https://doi.org/10.1089/cyber.2020.0299

Wisniewski, P., Ghosh, A. K., Xu, H., Rosson, M. B., & Carroll, J. M. (2017). Parental Control Vs. Teen Self-Regulation: Is There a Middle Ground for Mobile Online Safety? *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 51–69. https://doi.org/10.1145/2998181.2998352

Ziker, J. P., Fails, J. A., House, K., Boyer, J., Wendell, M., Abele, H., Maukar, L., & Ramirez, K. (2025). Parent-Child Adaptive Responses for Digital Resilience. *Social Sciences (2076-0760)*, *14*(4), 197. https://doi.org/10.3390/socsci14040197

## Appendix A

## Parental Control Features

Parental control features identified were classified into 8 categories. Seven categories followed a common monitor-restrict pattern and are listed in Table A1. The remaining category is defined by the logic or workflow to follow and is listed in Table A2.

**Table A1**

*Basic Parental Control Features Identified in Academic Literature*

| Identifier | Feature | Granularity |
|---|---|---|
| T | Time-based | |
| T1 | Manage usage based on time limit | Device, App, Website |
| T2 | Manage usage based on schedule by time of day | Device, App, Website |
| T3 | Manage usage based on schedule by day of week | Device, App, Website |
| T4 | Temporary access | Device |
| C | Content-based | |
| C1 | Manage content by category | App, Website |
| C2 | Manage content by site/app | App, Website |
| C3 | Manage dynamic and user generated content | App, Website |
| C4 | Restrict to curated content | Device, App, Website |
| N | Contact-based | |
| N1 | Manage text messaging contacts | Device |
| N2 | Manage social media contacts | App |
| N3 | Manage text messaging | Device |
| S | Sharing-based | |
| S1 | Manage social media activity | App |
| S2 | Approve social media activity | App |
| D | Physical and Device | |
| D1 | Manage macrolocation | Device, App |
| D2 | Manage microlocation | Device, App |
| D3 | Manage biometrics | Device |

| Identifier | Feature | Granularity |
|---|---|---|
| M | Monetary | |
| M1 | Manage software purchases | App |
| M2 | Manage marketplace purchases | App, Website |
| P | Connectivity | |
| P1 | Manage telephone calls | Device |

*Note.* Categories are denoted with a single letter identifier. Features are indented under their category.

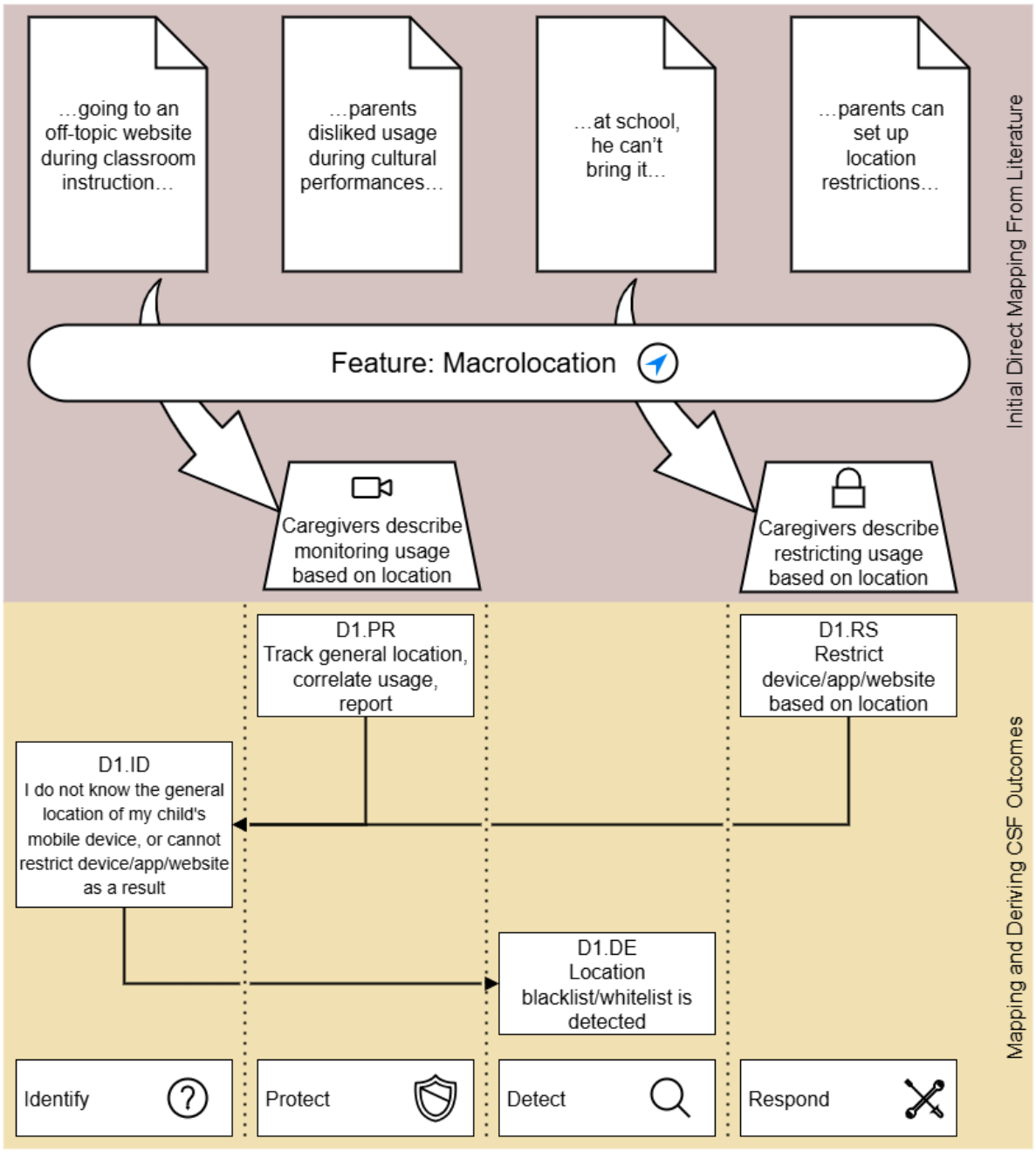
**Table A2**

*Logic-Based Parental Control Features (L) Identified in Academic Literature*

| Identifier | Feature | Granularity |
|---|---|---|
| L1 | Age-based rule adjustment | Rule, Rule Collection |
| L2 | Manage covert activity | Device, App, Website |
| L3 | Manage circumvention/malicious activity | Parental control system |
| L4 | Multi-featured rules | Rule collection |

## Appendix B

## Feature Mapping Example




*Note.* Example follows feature D1. Citations for top references, from left to right: Sweigart et al., 2025; Lukavská & Gabrhelík, 2024; Kotrla Topić et al., 2023; Sharma & Lee, 2024.

## Appendix C

## Catalog of Findings

| Identifier | Description | Type |
|---|---|---|
| T | Time-based | Category |
| T1 | Manage usage based on time limit | Feature |
| T1.ID | I do not know or cannot control how much time my child spends on device/app/website | Outcome |
| T1.PR | Record device/app/website usage, aggregate & report total time | Outcome |
| T1.DE | Usage surpasses target time limit | Outcome |
| T1.RS | Block device/app/website access after limit is reached | Outcome |
| T2 | Manage usage based on schedule by time of day | Feature |
| T2.ID | I do not know or cannot control my child's daily usage of device/app/website | Outcome |
| T2.PR | Record device/app/website usage, aggregate & report usage | Outcome |
| T2.DE | Usage occurs outside of daily schedule | Outcome |
| T2.RS | Block device/app/website access outside of schedule | Outcome |
| T3 | Manage usage based on schedule by day of week | Outcome |
| T3.ID | I do not know or cannot control when my child uses device/app/website | Outcome |
| T3.PR | Record device/app/website usage, aggregate & report usage | Outcome |
| T3.DE | Usage occurs outside of preset schedule | Outcome |
| T3.RS | Block device/app/website access outside of schedule | Outcome |
| T4 | Temporary access | Feature |
| T4.ID | I cannot stop access to device/app/website | Outcome |
| T4.PR | N/A | |
| T4.DE | N/A | |
| T4.RS | Parent sets timer, block device/app/website until timer completes | Outcome |

| Identifier | Description | Type |
|---|---|---|
| C | Content-based | Category |
| C1 | Manage content by category | Feature |
| C1.ID | I do not know or cannot control what types of sites my child sees on app/website | Outcome |
| C1.PR | Record app/website consumption, categorize endpoints, report by aggregation | Outcome |
| C1.DE | An endpoint in a category on a blacklist is accessed | Outcome |
| C1.RS | Block endpoint based on category | Outcome |
| C2 | Manage content by site/app | Feature |
| C2.ID | I do not know or cannot prevent if my child visits a specific app/website | Outcome |
| C2.PR | Record app/website consumption, report by each endpoint | Outcome |
| C2.DE | An endpoint on a blacklist is accessed | Outcome |
| C2.RS | Block endpoint | Outcome |
| C3 | Manage dynamic and user generated content | Feature |
| C3.ID | I do not know or cannot prevent what types of content my child sees on app/website | Outcome |
| C3.PR | Define model-aware classifications of interest, report when whitelist is triggered | Outcome |
| C3.DE | Blacklist image/text is detected | Outcome |
| C3.RS | Block content based on AI classification | Outcome |
| C4 | Restrict to curated content | Feature |
| C4.ID | I do not know when my child chooses curated content over open content. I cannot restrict app/website to only present curated content. | Outcome |
| C4.PR | Record approved curated providers, report when content consumed outside of approved list | Outcome |
| C4.DE | Content is consumed outside of approved curated content list | Outcome |
| C4.RS | Block content not on approved curated content list | Outcome |

| Identifier | Description | Type |
|---|---|---|
| N | Contact-based | Category |
| N1 | Manage text messaging contacts | Feature |
| N1.ID | I cannot review, restrict, or approve who my child is text messaging | Outcome |
| N1.PR | Access text messages, report on recipients | Outcome |
| N1.DE | Contact on blacklist is contacted | Outcome |
| N1.RS | Block message or request approval | Outcome |
| N2 | Manage social media contacts | Feature |
| N2.ID | I cannot review, restrict, or approve who my child is private messaging on social media | Outcome |
| N2.PR | Access private messages, report on recipients | Outcome |
| N2.DE | Contact on blacklist is contacted | Outcome |
| N2.RS | Block message or request approval | Outcome |
| N3 | Manage text messaging | Feature |
| N3.ID | I cannot read text messages or prevent the use of text messaging | Outcome |
| N3.PR | Access text messages, report on content | Outcome |
| N3.DE | Text message application/protocol is used | Outcome |
| N3.RS | Block text message application/protocol | Outcome |
| S | Sharing-based | Category |
| S1 | Manage social media activity | Feature |
| S1.ID | I do not know what my child is sharing/how my child is interacting online and cannot stop it | Outcome |
| S1.PR | Access social media posts, report on shared content and activity | Outcome |
| S1.DE | Blacklist of sharing action/behavior is detected | Outcome |
| S1.RS | Prevent blacklisted sharing action/behavior | Outcome |
| S2 | Approve social media activity | Feature |
| S2.ID | I cannot control what my child is sharing online | Outcome |
| S2.PR | Define model-aware classifications of interest, report when whitelist is triggered | Outcome |
| S2.DE | Blacklist image/text is detected | Outcome |
| S2.RS | Block activity or require approval based on AI classification | Outcome |

| Identifier | Description | Type |
|---|---|---|
| D | Physical and Device | Category |
| D1 | Manage macrolocation | Feature |
| D1.ID | I do not know the general location of my child's mobile device, and cannot restrict device/app/website as a result | Outcome |
| D1.PR | Track general location, correlate with device/app/website usage, report | Outcome |
| D1.DE | Location blacklist is detected | Outcome |
| D1.RS | Restrict device/app/website at location | Outcome |
| D2 | Manage microlocation | Feature |
| D2.ID | I do not know the specific location of my child's mobile device, and cannot restrict device/app/website as a result | Outcome |
| D2.PR | Triangulate specific location, correlate with device/app/website usage, report | Outcome |
| D2.DE | Location blacklist is detected | Outcome |
| D2.RS | Restrict device/app/website at location | Outcome |
| D3 | Manage biometrics | Feature |
| D3.ID | I cannot correlate or limit media use based on physical activity | Outcome |
| D3.PR | Monitor biometric data, correlate with device/app/website usage, report | Outcome |
| D3.DE | Blacklist of device/app/website during biometric activity is detected | Outcome |
| D3.RS | Restrict device/app/website until biometric signature changes | Outcome |
| M | Monetary | Category |
| M1 | Manage software purchases | Feature |
| M1.ID | I do not know or cannot prevent when my child purchases a new app | Outcome |
| M1.PR | Monitor app marketplaces for purchases | Outcome |
| M1.DE | Blacklist of app or app classification is detected | Outcome |
| M1.RS | Block app purchase | Outcome |
| M2 | Manage marketplace purchases | Feature |
| M2.ID | I do not know or cannot prevent when my child makes an online or in-app purchase | Outcome |
| M2.PR | Monitor purchases made against whitelist of marketplaces | Outcome |
| M2.DE | Blacklist of marketplace purchase is detected | Outcome |
| M2.RS | Block app/website purchase at marketplace | Outcome |

| Identifier | Description | Type |
|---|---|---|
| P | Connectivity | Category |
| P1 | Manage telephone calls | Feature |
| P1.ID | I cannot see what calls are made or received | Outcome |
| P1.PR | Access call log, report on activity | Outcome |
| P1.DE | N/A | |
| P1.RS | N/A | |
| L | Logic-based | Category |
| L1 | Age-based rule adjustment | Feature |
| L1.ID | I cannot automatically adjust rules based on my child's age | Outcome |
| L1.PR | Define rule profiles based on demographics | Outcome |
| L1.DE | Child's age changes, or virtual age/maturity level increases | Outcome |
| L1.RS | Automatically apply new rule profile | Outcome |
| L2 | Manage covert activity | Feature |
| L2.ID | I do not know when my child is trying to hide online activity, and cannot change rules appropriately | Outcome |
| L2.PR | Define conditions for covert activity, report | Outcome |
| L2.DE | Covert activity is detected | Outcome |
| L2.RS | Temporarily block all activity based on timer or schedule | Outcome |
| L3 | Manage circumvention/malicious activity | Feature |
| L3.ID | I do not know when my child is trying to circumvent parental controls, and cannot do anything about it | Outcome |
| L3.PR | Record activity metrics through redundant systems | Outcome |
| L3.DE | Anomalous activity is detected | Outcome |
| L3.RS | Temporarily block all activity based on timer or schedule | Outcome |
| L4 | Multi-featured rules | Feature |
| L4.ID | Restrictions are not smart enough | Outcome |
| L4.PR | Allow complex rule sets based on multiple conditions | Outcome |
| L4.DE | N/A | |
| L4.RS | Allow complex rule sets based on multiple conditions | Outcome |

*Note.* N/A indicates an outcome was not applicable to the risk identified. The CSF function remains listed in the table for completeness.