Evaluation of Parental Control Tools Functionalities: The Chilean Context

Nicolás Rojas
Nicolás Boettcher
Pablo Palacios Játiva
Miguel Gutiérrez Gaitán*

*CISTER Research Centre

CISTER-TR-240801

2024/10/21

Evaluation of Parental Control Tools Functionalities: The Chilean Context

Nicolás Rojas, Nicolás Boettcher, Pablo Palacios Játiva, Miguel Gutiérrez Gaitán*

*CISTER Research Centre

Polytechnic Institute of Porto (ISEP P.Porto)

Rua Dr. António Bernardino de Almeida, 431

4200-072 Porto

Portugal

Tel.: +351.22.8340509, Fax: +351.22.8321159

E-mail: nicolas.boettcher@mail.udp.cl, mjggt@isep.ipp.pt

https://www.cister-labs.pt

Abstract

Choosing a reliable parental control tool is essential to supervising minors accessing information and using electronic devices. For this, it is necessary to determine which tools are the most suitable and if their functionalities are effective. To our knowledge, despite the availability of existing tools that evaluate applications and different actors, e.g., parent control applications recommended by Internet Service Providers (ISPs), none of them properly characterize the various functionalities provided by the application while validating their efficacy. In this paper, we propose a new comprehensive metric to effectively identify and evaluate the functionalities provided by tools in the field of parental control. The metric is applied to some of the most downloaded apps from the Play Store, and the results are compared with the applications recommended by ISPs in Chile, which cover more than 93% of the market. The results from our analysis show that none of the parent control applications recommended by Chilean ISPs managed to provide full confidence in the functionalities implemented since at least one of their functions did not pass the test applied. The end goal for the test metric proposed is to allow future developers to assess their applications beforehand while offering a better match with the customer 19s expected service.

Evaluation of Parental Control Tools Functionalities: The Chilean Context

Nicolás Rojas[1], Nicolás Boettcher[1], Pablo Palacios Játiva[1], and Miguel Gutiérrez Gaitán[2]

[1] Universidad Diego Portales, Chile
{nicolas.rojas_f,nicolas.boettcher,pablo.palacios}@mail.udp.cl
[2] Pontificia Universidad Católica de Chile, Chile
{miguel.gutierrez}@uc.cl
[3] CISTER Research Centre, Porto, Portugal
{mjggt}@isep.pt

Abstract. Choosing a reliable parental control tool is essential to supervising minors accessing information and using electronic devices. For this, it is necessary to determine which tools are the most suitable and if their functionalities are effective. To our knowledge, despite the availability of existing tools that evaluate applications and different actors, e.g., parent control applications recommended by Internet Service Providers (ISPs), none of them properly characterize the various functionalities provided by the application while validating their efficacy. In this paper, we propose a new comprehensive metric to effectively identify and evaluate the functionalities provided by tools in the field of parental control. The metric is applied to some of the most downloaded apps from the Play Store, and the results are compared with the applications recommended by ISPs in Chile, which cover more than 93% of the market. The results from our analysis show that none of the parent control applications recommended by Chilean ISPs managed to provide full confidence in the functionalities implemented since at least one of their functions did not pass the test applied. The end goal for the test metric proposed is to allow future developers to assess their applications beforehand while offering a better match with the customer's expected service.

Keywords: Parental control · Android · PDNS · Application evaluation

1 Introduction

Currently, we are facing a global-level problem. The uncontrolled use of mobile devices by children and adolescents (CA), along with the lack of supervision by their guardians, parents, or caregivers (GPC), has resulted in the emergence of various disorders, such as lack of sleep [4], gaming disorders [6], among others. As a result, protecting the CA from exposure to these devices becomes relevant. Globally, the US and the EU have been major references in the protection of minors, regulating the content that CA can access, and restricting their access to categories of sites such as weapons, gambling, and pornography, among others. Reports in Chile indicate that the time spent in front of screens by minors between 9 and 12 years of age exceeds 3 hours a day [5, 11], and it is observed that they engage in mainly digital activities without time restrictions and adult supervision. A similar result is found in [21], which shows that 42% of US children aged 4 to 14 spend more than 30 hours a week on their phones (or their parents' phones). Among the mechanisms developed to protect CA are website restrictions through Protective DNS (PDNS) [15] and parental control tools [27], which help GPC to control CA's screen time [26]. Due to the importance of such tools, they have been analyzed from various perspectives, such as cybersecurity, psychology, and sociology [2, 8, 16, 25], without having evidence – to our knowledge – of a mechanism that evaluates the functionalities of mobile applications in the domain of parental control and compares them with existing metrics. However, if a functionality fails to fulfill its purpose, it is sufficient to determine that it is not a suitable tool for GPC to place its trust in. Moreover, even if at the public policy level Chile was the first country in the world to stipulate in its net neutrality law an obligation to ISPs to provide a parental control service available to users who require and request that blocks content contrary to the law, morals, or good moral [9], a relatively recent study [5], reveals that 12 years after the promulgation of that law, only 37% of respondents are aware of parental control tools, yet not necessarily aware of their effectiveness.

In this work, we will introduce a novel metric to evaluate different tools functionalities comprehensively and thus determine the effective level of parental control offered by the ISPs parent-control tools available in Chile. The rest of this paper is organized as follows: in the next section, related work is presented to highlight ways to protect CA from inappropriate content. Then, Section 3 presents the parental control functions studied, and Section 4 presents the analysis and results obtained. Finally, Section 5 concludes the paper.

2 Related works

To date, multiple parental control tools for mobile devices provide similar functionalities and features without a formal mechanism to identify how they differ. There are PDNS, which provide name resolution services specialized in blocking content by categories such as ads and adult content, among others. These services can be configured at the network or device level. Unfortunately, they are limited to filtering content, fulfilling only part of the functionalities provided by parental control tools. As a result, selecting the best parental control tool becomes complex, especially if evaluation systems mix objectivity of only some features or are based on subjective user opinions, such as those from the Android Play Store [22]. To address this, in [10], parental control tools are evaluated based on compatibility, customization, ease of installation, price, and types of blocking. However, comparative evaluation sites, such as IS4K [19] and more exhaustive ones, such as SIP-BENCH III [1], provide detailed information on parental control tools, focusing on various dimensions such as the platform on which they operate, price, language, efficiency, usability, security, and functionality. In this last category, different areas are developed in detail, indicating mechanisms to evade their functionalities. Among the various functionalities, filters based on different categories or through URL lists (whitelist or blacklist) are indicated. Blocking messages is also considered, reinforcing studies focused on cyberbullying, which demonstrate that the best way to prevent these situations is to restrict who the CA is communicating with [3]. Despite the extensive information collected, the analyzed applications are over eight years old, some evaluated techniques are deprecated, and they do not consider functionalities like device geolocation, a widely used feature today. In recent studies of parental control applications, it has been evidenced that research lines have focused on the protection of private data [20], without finding studies that have continued the line of evaluating the functionalities of these tools. This is concerning, given the high dynamism of Internet content and the importance given to content categorization in parental control tools. Tom's Guide, a specialized benchmarking site [24], conducted a comparison of the best parental control tools for mobile devices for the year 2024. Applications are evaluated on a scale of up to five stars, emphasizing the options each tool contains and the user experience. To our knowledge, the processes performed to assess the applications or the functions evaluated are not evident. Among the apps analyzed in that study, Qustodio is chosen as the best monitoring application, despite 7% of the comments on the Play Store [22] indicating that its restrictions are easy to bypass.

3 Parental Control Functions

For a thorough evaluation, we selected the parental control applications through the Android Play Store, with a restriction on those that had more than one million downloads. The decision to choose Android over iOS, or both, was influenced by users' perception of preferring higher-ranked applications. In [13], a study conducted on cross-platform applications, it was revealed that Android users tend to give higher ratings compared to iOS users. This trend suggests that Android users may be less likely to notice or report functionality issues within applications on this operating system.

To ensure a comprehensive analysis, we requested trial versions of the paid apps from each developer. We specifically chose not to rely on user opinions or AI-driven evaluations in our selection of parental control apps for several critical reasons. First, user reviews often contain subjective biases, as they are influenced by individual experiences that may not be representative of the broader user base. These reviews can also be disproportionately negative or positive based on temporary issues or personal preferences that do not necessarily reflect the app's overall performance or suitability for all users [7]. Furthermore, AI systems that analyze user reviews to make recommendations can inadvertently amplify these biases. These systems are often trained on datasets that reflect existing societal biases and subjective opinions, leading to skewed results that do not accurately capture the true effectiveness of an app. AI-driven evaluations can misinterpret the context of user reviews, leading to flawed decision-making where certain apps may be unfairly favored or dismissed [14]. By directly testing trial versions of applications, we can ensure that our analysis is based on objective criteria and first-hand experience, free from the distortions that might be introduced by user opinions and AI recommendations. This approach allows us to provide a more accurate and fairer assessment of parental control apps, ensuring that our recommendations are based on reliable and unbiased data.

In Table 1, the ID associated with each analyzed application can be seen, along with the number of downloads detected to date, according to the geographical location of the United States. Furthermore, in Table 2, the parental control applications offered by the ISPs in Chile, covering more than 93% of the Chilean customer market [23], are reported, indicating which parental control tool they offer their customers.

Table 1. Parental control applications for Android.

#	Name	ID	Version	Downloads
1	Qustodio	com.qustodio.family.parental...	182.14.1	more than 1 million
2	Kaspersky	com.kaspersky.safekids	1.88.0.9	more than 1 million
3	Norton	com.symantec.familysafety	7.2.0.19	more than 1 million
4	OurPact	com.ourpact.androidparent	1.0.29	more than 1 million
5	Screen Time	com.screentime.rc	3.11.68	more than 1 million
6	ESET	com.eset.parental	5.1.6.0	more than 1 million
7	FamiSafe	com.wondershare.famisafe	6.2.6	more than 5 millions
8	Microsoft	com.microsoft.familysafety	1.24.0.941	more than 1 million
9	Google	com.google.android.apps.kids...	2.4.0.H...	more than 50 millions

Table 2. Parental control tools offered by Chilean ISPs and their market share.

ISP	**Parental Control tool**	**Market Share**
Movistar	Qustodio	30.7%
VTR	VTR Play	23.9%
Claro	Norton	6.8%
Mundo	Qustodio	18.4%
Entel	Google, Kaspersky	7.1%
GTD	Eero Secure	7%

Then, to identify the functionalities that represent the majority of these types of applications, each selected application was analyzed in search of functional requirements associated with parental control. In this process, usability, presentation, and agility, among others, were excluded from the evaluation, highlighting the functionalities of restricting, protecting, and alerting, as they are fundamental for the CA's supervision. We will use the designations of client and server devices to refer to the devices used by the CA and that of the GPC. The categories of functionalities evidenced in [1] were complimented, and for each of them, a test environment was defined to specify how each functionality is evaluated. The ten generated functions are detailed below:

1. **Filter:** Function that allows blocking websites by categories. To evaluate the effectiveness of this function, the sites mentioned in Table 3 are used. After activating content filters for gambling, weapons, and violence on the client device, the sites are accessed through the browser URL. If all websites are blocked, a ✓ is recorded; otherwise, a ✗.
2. **Real-time Blocking:** Function that enables real-time changes on the client. In case of blocking an application in use on the client and identifying its instantaneous blocking, a ✓ is recorded; otherwise, a ✗. If an application used on the client device is blocked and its instant block is identified, a ✓ is recorded; otherwise, an ✗ is recorded.
3. **Airplane Mode:** Function that identifies if it is feasible to bypass restrictions on the client by eliminating connectivity between the client and the server. Airplane mode is activated on the client device, and general-use applications (defined in Sec. 3.1) are executed to avoid sending reports to the server, allowing their use without server approval. If the general-use application cannot be used in airplane mode, a ✓ is recorded; otherwise, a ✗.
4. **App Monitoring:** Function that informs the server which application is running. If the notification is received on the server as soon as an application is executed on the client device, a ✓ is recorded; otherwise, a ✗.
5. **Chat Monitoring:** Function that monitors social media messaging applications and generates reports based on keywords. Social media applications were used to send messages to the client's device. To test the alarm, the following keywords were used: ”te tiraste”, ”tunazo”, ”wn”, ”camotazo”, which are used in contexts of violence and weapons. These words are not commonly known by the entire Chilean population, as slang varies between different generations [18]. If messages containing the keywords are recorded, a ✓ is recorded; otherwise, a ✗.
6. **Call Monitoring:** Function that blocks incoming calls. Calls are made to the client device from an unregistered number. If the incoming call is identified as unknown and its blocking is allowed, a ✓ is recorded; otherwise, an ✗ is recorded.
7. **Timer:** Function that restricts the usage time of both the device and client applications. An attempt was made to modify the time on the client device to have more time than stipulated by the server. If authorization from the server is required to change the time, a ✓ is recorded; otherwise, a ✗.
8. **Calendar:** Function that restricts the usage days of the client device. An attempt was made to modify the date on the client device to have more days than stipulated by the server. If server permissions are required to change the date on the client device, a ✓ is recorded; otherwise, a ✗.
9. **Geolocation:** Function responsible for generating reports on the real-time location of the client device. To verify the accuracy of this function, a GPS

spoofer was used to generate a false location. If a notification is received on the server when attempting to modify the geolocation, a ✓ is recorded, otherwise a ✗.

10. **Geofence:** Function that identifies if the client device has left a safe area (an area previously defined by the GPC). This functionality is especially important when emphasizing the accuracy of the GPS application [12], which is known to be not entirely accurate in parental control applications. A GPS faker was used to simulate leaving the safe area, and the safe zone's limit radius was exceeded by 200 meters. If a notification informs that the client device is outside the safe zone, a ✓ is recorded; otherwise, a ✗.

Based on the identified functionalities, we propose the Functionality Index (FI) as an integrated metric corresponding to the sum of the values recorded for each of the ten functionalities. If a ✓ is obtained, it is assigned a value of 1, otherwise a value of 0. The total value is converted to a scale of 1 to 5 stars to compare it with the Play Store's scoring system and Tom's guide.

$$\mathrm{FI} = \frac{4}{10}\sum_{i=1}^{10} F_i + 1 \tag{1}$$

where F_i corresponds to the value recorded in the i-th function.

3.1 Evaluation Environment

To evaluate the functionalities of parental control applications, an environment with Windows 10 was used, with the client and the server running Android 11 on the Android Bluestacks 5 emulator. Google Chrome version 110.5481.154 was used as the Internet browser, Viber Messenger version 19.5.4.0 as the messaging and calling software, and FakeGPS version 2.1.2, selected as the best application to spoof the client's location in [17]. To evaluate the different functionalities of parental control tools, CA defined general-use applications. Among these applications, we found the most downloaded games according to the Play Store and the most used Internet apps by CA. We used Free Fire, Roblox, Ultimate Guys, YouTube, Snapchat, Instagram, TikTok, and Facebook for this work. Filters associated with adult content were tested using weapons and online casino sites. For each site, it was verified through the PDNS services reported in [15], which offer blocking and filtering of ad messages of adult content if it is feasible to identify that they belong to categories not suitable for minors and to deny their resolution of name. Table 3 lists the sites and PDNS services used, where a ✓ was recorded if the site was blocked by the PDNS, otherwise an ✗.

4 Analysis and Results

For each application in Table 1, the ten identified functions were evaluated, and based on the results, Table 4 was built. If the functionality could not be

Table 3. Sites with content not suitable for minors.

URL	Type	Adguard DNS	ControlID DNS	OneDNS	114DNS	SafeSurfer
www.betsson.com/cl/casino	Casino	✗	✗	✗	✗	✗
www.mbitcasino.io/	Casino	✗	✗	✗	✗	✗
www.ignitioncasino.eu/	Casino	✗	✗	✗	✗	✗
www.impactguns.com/	Guns	✗	✗	✗	✗	✗
www.operationmilitarykids.org	Guns	✗	✗	✗	✗	✗
www.navysealmuseum.org/	Guns	✗	✗	✗	✗	✗
www.gunsamerica.com/	Guns	✗	✗	✗	✗	✗
www.mccoyoutdoorco.com/	Guns	✗	✗	✗	✗	✗
www.greentophuntfish.com/	Guns	✗	✗	✗	✗	✗

evaluated because it was only available in the full version and was not in the trial version provided by the developer, it was recorded with an F. It was considered to have a score of 0. Despite PDNS claiming to be capable of filtering adult sites, it was found that they did not manage to block the sites indicated in Table 3. However, based on the data obtained in Table 4, five of the parental control applications were able to detect them completely using category filters. Although we have not evaluated filtering by specific URLs, it is important to note that only Kaspersky and Google allow the use of blacklists to filter sites. As observed, most of the functionalities recorded with an F correspond only to chat monitoring, call monitoring, and GPS usage, allowing the use of the rest of the basic functions. Filter and Geofence are among the functions with the highest ✗ records. As expected, the Filter is one of the most demanding fields since it depends on large, updated databases, either to detect or train different learning models. However, the accuracy of the geolocation tool is essential to achieve the proper functionality. Based on the collected data, the FI value was calculated to compare the scores obtained in the Play Store and Tom's Guide. No comparison was made with the scores of SIP-Bench III since they correspond to versions older than eight years.

In Table 2, the parental control applications offered by ISPs in Chile to comply with the law on net neutrality are reported. It is observed that Movistar and Mundo together cover more than 49% of the telecommunications market share in Chile. Both offer Qustodio as a parental control application, which, together with the rest of the applications, based on the evidence in Table 4, except for ScreenTime, proves to be unable to meet at least one functionality, validating the feasibility of bypassing the restrictions reported in [22]. In other words, it shows the existence of at least one x in one of its functionalities. Based on the data obtained from Fig. 1, it is found that Qustodio, although the highest-rated application in the Play Store, scores only 3 points with FI, placing it below average. In contrast, Famisafe, the lowest-rated tool in the Play Store, achieved the highest score through FI.

Table 4. Evaluation of the functionality for each application.

ID	Filter	Real-time Blocking	Airplane Mode	App Monitoring	Chat Monitoring	Call monitoring	Timer	Calendar	Geolocation	Geofence
1	✓	✓	✗	✓	F	F	✓	✓	F	F
2	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗
3	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
4	✗	✗	✓	✓	F	F	✓	✓	✗	✗
5	✓	✓	✓	✓	F	F	✓	✓	F	F
6	✗	✓	✓	✓	F	F	✓	✓	F	F
7	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
8	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
9	✓	✓	✗	✓	✓	✓	✓	✓	✗	✗

Norton was the only tool that managed to alert the client when the device left the safe zone. Meanwhile, VTR uses a parental control tool to restrict access to its multimedia service, and GTD uses a tool that communicates directly with the router it provides. Both are limited to restricting content using their infrastructure, so we do not consider them in this study. Finally, Entel is the only ISP that recommends more than one parental control tool, making it clear in its terms and conditions that they are not part of the service.

According to the findings from Tom's guide, most applications garnered similar ratings, with Kaspersky being the exception, earning the highest score. Notably, the functions of the applications did not show any significant disparities.

5 Conclusions

While numerous parental control tools are available, the lack of a formal mechanism to objectively evaluate them, considering all their features, poses a significant risk to the current state of Internet safety. In this work, we identify the most downloaded mobile parental control applications on the Play Store and many PDNS specialized in blocking adult content. Based on filter functionality, we could show that despite using specialized tools to detect adult content, not all managed to block it. This highlights the need for further research in this area, considering the high dynamism of Internet content and the negative effects that the mass adoption of AI may bring. Based on our results, parental control tools will have a higher priority over PDNS if we need to filter the content by categories. From several scoring mechanisms evaluated, it is observed that there is a feature diversity to consider in these metrics, complicating the choice of the GPC of the best tool for supervising the CA. Our work shows that not all functionalities, just because they are present or declared, function correctly, which is what the GPC would expect. The problem of offering the best tool is accentuated

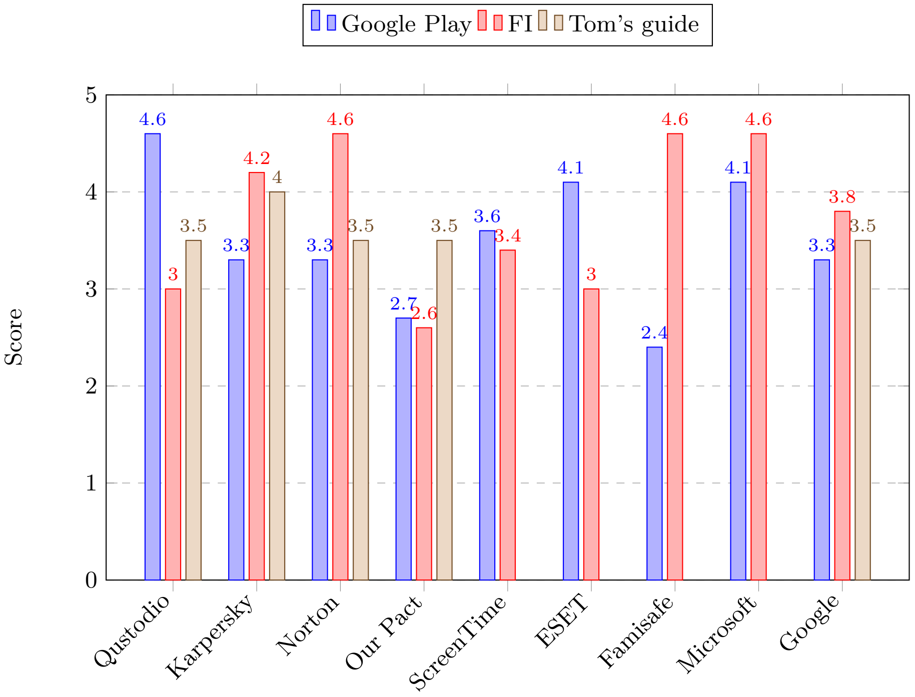

Fig. 1. Comparison of different evaluation metrics.

when Internet operators offer solutions that are not optimal. Our findings reveal a significant limitation in the current state of parental control tools. All the applications offered by ISPs in Chile, among those analyzed, did not demonstrate the correct functioning of at least one functionality of the parental control tools. This underscores the pressing need for innovation and improvement in this area. This leaves the investigation open to continue to seek mechanisms that allow for more precise evidence of whether the functionalities provided by parental control tools effectively meet what is stipulated.

Acknowledgements This research was supported by FONDECYT Regular 1211132, FONDECYT Iniciación 11240799, FONDECYT Iniciación 11241221, ANID PFCHA/Beca de Doctorado Nacional/2019 (21190489), SENESCYT ”Convocatoria abierta 2014-primera fase, (Acta CIBAE-023-2014)” and Escuela de Informática y Telecomunicaciones, Universidad Diego Portales; also by the CISTER Research Unit (UIDP/UIDB/04234/2020) through FCT/MCTES (Portuguese Foundation for Science and Technology) National Funds.

References

1. SIP Benchmark III. Safer Internet Programme (2017), https://www.sipbench.eu/index.cfm/secid.7/secid2.4, last accessed 2023/06/06
2. Ali, S., Elgharabawy, M., Duchaussoy, Q., Mannan, M., Youssef, A.: Betrayed by the guardian: Security and privacy risks of parental control solutions. In: Proceedings of the 36th Annual Computer Security Applications Conference. p. 69–83. ACSAC '20, Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3427228.3427287
3. Baldry, A.C., Sorrentino, A., Farrington, D.P.: Cyberbullying and cybervictimization versus parental supervision, monitoring and control of adolescents' online activities. Children and Youth Services Review **96**, 302–307 (2019)
4. Bernardi, G.I., et al.: Problematic internet use in children and adolescents: associations with psychiatric disorders and impairment. BMC Psychiatry **20**(1), 252 (2020). https://doi.org/10.1186/s12888-020-02640-x
5. Black & White, Ripley: Informe de Resultados Padres, madres y su relación con el ciberacoso. (2022)
6. Cho, K., Kim, M., Cho, Y., Hur, J.W., Kim, D.H., Park, S., Park, S., Jang, M., Lee, C.G., Kwon, J.S.: Digital phenotypes for early detection of internet gaming disorder in adolescent students: Explorative data-driven study. JMIR Mental Health **11**, e50259 (Apr 2024). https://doi.org/10.2196/50259
7. Fayyaz, Z., Ebrahimian, M., Nawara, D., Ibrahim, A., Kashef, R.: Recommendation systems: Algorithms, challenges, metrics, and business opportunities. Applied Sciences **10**(21) (2020). https://doi.org/10.3390/app10217748, https://www.mdpi.com/2076-3417/10/21/7748
8. Feal, , Calciati, P., Vallina-Rodriguez, N., Troncoso, C., Gorla, A.: Angel or devil? a privacy study of mobile parental control apps. Proceedings on Privacy Enhancing Technologies **2020**(2), 314–335 (Apr 2020). https://doi.org/10.2478/popets-2020-0029
9. Fuenzalida Hurtado, C.: Diez años de la neutralidad de la red en Chile: historia, análisis de su regulación y jurisprudencia (2020)
10. Fuertes, W., Quimbiulco, K., Galárraga, F., García-Dorado, J.L.: On the development of advanced parental control tools. In: 2015 1st International Conference on Software Security and Assurance (ICSSA). pp. 1–6. IEEE (2015)
11. Fundación para la Convivencia Digital y Centro de Investigación de Salud Mental Estudiantil de la U. de los Andes: Estudio: Percepción de riesgo y supervisión parental frente al uso de tecnologıas en menores de 13 años 2021-2022 (2022)
12. Gilmore, J.N.: Securing the kids: Geofencing and child wearables. Convergence **26**(5-6), 1333–1346 (2020)
13. Hu, H., Wang, S., Bezemer, C.P., Hassan, A.E.: Studying the consistency of star ratings and reviews of popular free hybrid android and ios apps. Empirical Software Engineering **24**(1), 7–32 (2019). https://doi.org/10.1007/s10664-018-9617-6, https://doi.org/10.1007/s10664-018-9617-6
14. Kadiresan, A., Baweja, Y., Ogbanufe, O.: Bias in AI-Based Decision-Making, pp. 275–285. Springer International Publishing, Cham (2022). https://doi.org/10.1007/978-3-030-84729-6_19, https://doi.org/10.1007/978-3-030-84729-6_19
15. Liu, M., Zhang, Y., Li, X., Lu, C., Liu, B., Duan, H., Zheng, X.: Understanding the implementation and security implications of protective dns services (2024)

16. Lundberg, J., Marklund, O.: ADOLESCENTS IN CONTROL: Promoting Adolescents Autonomy in Parental Control Applications. Master's thesis, Department of Informatics, Human Computer Interaction and User Experience (August 2023)
17. MakeUseOf: The 7 best free android apps to fake your gps location (nov 2022), https://www.makeuseof.com/best-android-location-spoofing-apps/, last accessed 2023/06/06
18. Marca Chile: Modismos Chilenos de la A a la Z (November 2017), https://www.marcachile.cl/modismos-chilenos-de-la-a-a-la-z/, last accessed 2023/06/06
19. Núñez-Gómez, P., Ortega-Mohedano, F., Monguí Monsalve, M., Larrañaga, K.: El consumo y uso de dispositivos móviles y Apps por los niños y las niñas de la generación Alpha en España. Internet Seguro For Kids (IS4K). INCIBE (2020)
20. de Paula Albuquerque, O., Fantinato, M., Hung, P.C., Peres, S.M., Iqbal, F., Rehman, U., Shah, M.U.: Recommendations for a smart toy parental control tool. The Journal of Supercomputing **78**(8), 11156–11194 (2022)
21. Sellcell: Kids cell phone use survey 2019-truth about kids & phones (2019), https://www.sellcell.com/blog/kids-cell-phone-use-survey-2019/, last accessed 2023/06/06
22. Stoev, M., Sarmah, D.K.: Online protection for children using a developed parental monitoring tool. In: International Congress on Information and Communication Technology. pp. 205–215. Springer (2023)
23. Subsecretaría de Telecomunicaciones de Chile: Cierre año 2023 (2024), https://www.subtel.gob.cl/wp-content/uploads/2024/04/Informe-telecomunicaciones-Dic23.pdf, last accessed 2023/06/06
24. Tom's Guide: The best parental control apps for android and iPhone 2023 (feb 2023), https://www.tomsguide.com/us/best-parental-control-apps,review-2258.html, last accessed 2023/06/06
25. Wang, G., Zhao, J., Van Kleek, M., Shadbolt, N.: Protection or punishment? relating the design space of parental control apps and perceptions about them to support parenting for online safety. Proceedings of the ACM on Human-Computer Interaction **5**(CSCW2), 1–26 (Oct 2021). https://doi.org/10.1145/3476084
26. Wang, H., Tong, L.: Association between screen time and internalizing and externalizing behavioral problems in primary and secondary school students in shanghai. Chinese Journal of School Health **45**(4), 514–519 (2024). https://doi.org/10.16835/j.cnki.1000-9817.2024128
27. Wisniewski, P., Ghosh, A.K., Xu, H., Rosson, M.B., Carroll, J.M.: 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. p. 51–69. CSCW '17, ACM (Feb 2017). https://doi.org/10.1145/2998181.2998352