Do Platforms Care About Your Child's Data? A Proposal of Legal Requirements for Children's Privacy and Protection

George Valença[1], Maria Wanick Sarinho[2], Vinícius Polito[1], and Fernando Lins[1]

[1] Dpto de Computação, Universidade Federal Rural de Pernambuco, Brasil
[2] Centro de Ciências Jurídicas, Universidade Federal de Pernambuco, Brasil
{george.valenca,vinicius.polito,fernandoaires}@ufrpe.br,
mariasarinho@ufpe.br

Abstract. To promote children's data protection, the design of services and products matters, as well as continued enforcement of terms of use and privacy policies by tech companies. However, the child, their rights and Privacy by Design principles place the burden on platforms to develop age-appropriate and rights-oriented experience. To highlight the duties of Big Techs and guide them in implementing children's privacy and data protection, we present 19 legal requirements (LR) based on UNICEF's Manifesto and the standard Children's Right by Design. Besides, to illustrate how each LR can be implemented, we consider examples from Youtube Kids and TikTok platform ecosystems. Our goal is to pave the way for a shift towards children's protection and promotion by tech companies, reducing the detrimental use of their data.

Keywords: Privacy · Legal Requirements · Children's rights

1 Introduction

An estimated one in three internet users globally is a child. In the global South, this number is even higher and children lead the way in the adoption of new technologies as they are online more time than adults [11]. The combination of early access and widespread use of mobile devices raises important questions about platform's design and business models, parental support and mediation of a child's use of social media platforms. Recently, UNICEF revealed children are (i) less concerned about certain aspects of online privacy than adults and (ii) less able to understand and mitigate privacy-related risk [11]. It proposes the *"recognition of children's rights should be embedded in the activities, policies and structures of Internet governance processes"*. The United Nation's Convention on the Rights of the Child (CRC) introduces the child's best interests and right to privacy (Art. 16) as a basic tenet to be observed as a *"primary consideration"* by stakeholders in the public and private sector [1], which was reinforced by the most recent General Comment n. 25 from the CRC Committee.

However, these aspects continue to be largely side-lined by ecosystems raised around Big Techs' platforms. Instagram rely on a high referent power to have

users consenting to its terms of use, privacy policies and data protection practices [18]. Hence, we perceive a growing scrutiny over how these platforms deal with children's data and if their measures to guarantee children's best interests and rights are effective. Another example is the thriving platform ecosystem established by the Chinese firm ByteDance: TikTok. This ecosystem, which is formed by a multitude of users and advertisers, figures in the top-3 favorite platforms for children, with around 18 million users aged 14 and under in the US [7]. Despite the prevalence of children in its base, TikTok's initiatives seem insufficient to protect such vulnerable and highly connected users [2, 3, 19].

This setting motivated us to investigate the following research question (RQ): *are the measures taken by software platforms effective in light of legal requirements for children's privacy and data protection?* To answer this RQ, we considered the Children's Rights-by-Design (CRbD) standard for data use by tech companies, which details the CRC for designers and developers. We translated the CRbD standard into 19 legal requirements (LR) that enable the protective governance of children's data by a company. To illustrate the implementation of these LRs, we use examples from TikTok and Youtube Kids ecosystems, whose customer base is largely formed by children. Our main goal is guiding platform companies in developing products and services that protect children online.

2 Power and Privacy in Platform Ecosystems

Tech companies have shifted to complex ecosystems, in which businesses work as a unit in a shared market via a platform (e.g. Amazon's Alexa) [22]. In the age of Surveillance Capitalism, a power asymmetry between users and platform companies causes an amalgamation of data from individuals being used to predict and influence user behaviour as well as to inform business decisions [10]. The power from Big Tech ecosystems, a widespread public perception of significant privacy risks in online activity, and a need for uniform rules led to the creation of data protection laws around the globe [18]. Such power asymmetry is higher when the user is a child (*"a human being below the age of 18 years unless under the law applicable to the child, majority is attained earlier"* - CRC). Data protection laws and standards claim prevention is needed in ecosystems, which gain competitive advantage by adopting Privacy by Design (PbD).

In the EU, the General Data Protection Regulation (GDPR) implements Privacy by Design (PbD) to integrate the necessary safeguards into the processing with prevention in mind. PbD is formed by 7 foundational principles that put privacy at the center to ideally become an organization's default mode of operation [5]. They are (i) proactive not reactive, (ii) privacy as the default setting, (iii) privacy embedded into design, (iv) full functionality, (v) end-to-end security, (vi) visibility and transparency, and (vii) respect for user privacy.

The principle (i) (*"proactive not reactive"*), for instance, states compliance with regulatory frameworks alone is unsustainable as the sole model for ensuring the future of privacy. Instead, prevention is needed in platform ecosystems. Building privacy into the platform creates a competitive advantage and

yields many benefits, ranging from cost-savings, to strengthen consumer relationships. The CRC treaty uses these principles by focusing on prevention and on a positive-sum approach to privacy and data protection regarding children to promote children's rights and development as well as to protect them from violations regarding the detrimental use of their data [9].

3 Legal Requirements for Children's Privacy and Protection by Platform Companies

To provide greater practical application, we translate the CRC standard for children's data use by tech companies into legal requirements for platform designers and developers. We group these LRs in three categories: *company governance* (Section 3.1), *product or service development* (Section 3.2), and *product and service provision* (Section 3.3), similarly to the CRbD [9]. Hence, we describe and exemplify tech companies' duty under the CRC articles.

3.1 Company Governance

Ecosystems must incorporate the CRC for children's rights as internal policy across all sectors. Hence, **companies shall integrate the CRC provisions into all appropriate platform policies and management processes** (LR1) related to the design and development of products and services (e.g. new features, apps). For instance, TikTok recently stated it had *"robust policies, processes and technologies in place to help protect all users, especially teenage users"* [20].

Besides, **companies shall adopt an interdisciplinary perspective on platform development to achieve the best interests of the child** (LR2). This can be accomplished by incorporating the opinion of children and families, and the perspectives of experts for platform evolution - e.g. TikTok announced plans to bring in European experts in fields such as child safety, young people's mental health and extremism [13]. In an ecosystem, **companies shall adopt the best technologies and policies available for platform development universally** (LR3) in all countries where it is available. For example, Google rolled out several changes on Youtube Kids globally - e.g. restricting access to adult content by enabling its SafeSearch filtering technology by default to all users under 13 [15]. Also, **companies shall conduct due diligence of platform policies** (LR4) to enforce their terms and community standards, especially regarding privacy policies and age verification. An example of conformance with this requirement is TikTok's Community Guidelines Enforcement Report, which informs how its policies have been applied to protect under-age users [21].

3.2 Product or service development

UNICEF recommends that **companies shall consider data minimisation** (LR5), when all children's data processed by the platform should be adequate, relevant and not excessive. Their **platforms need to enable children's full**

control of their data (LR6), providing minors and families with online tools to easily access, ratify, erase, restrict or object to processing their data. Given the general concern with data processing practices, Google required app developers to disclose how their solutions collect and use data [15]. Besides, the Big Tech created the website *Family Link privacy guide for children & teens*, which describes for parents and guardians whatdata it collects in association with their child's Google Account [8]. It also enables a child to change some of the information saved by the platform (e.g. disabling YouTube History feature). On TikTok, users from 16 to 17-years-old can specify who they want to share videos with [6].

In ecosystems, **companies shall provide commercial-free digital spaces** (LR7) on their platforms by avoiding children's nudge techniques, microtargeting of advertising and data monetisation via profiling. Besides, to prevent the exploitation of children's images or artistic expression, **companies shall offer meaningful and non-monetisable experiences in the platform** (LR8). These requirements were recently addressed by YouTube, which reduced *"overly commercial content"* from YouTube Kids. To stop encouraging kids to spend money, this ecosystem has removed the popular "unboxing" videos, which glamorise product packaging and turn unknown users into famous youtubers [15].

As **companies shall ensure to use nudge techniques in the best interest of the child** (LR9), they foster children's development with transparency and ethics. To safeguard against the improper exposure of children's data and persistent identifiers that facilitate non-authorised and malicious contact within their platforms, **companies shall adopt safety standards on platform development** (LR10). Hence, they avoid and combat child sexual abuse material. After being accused of providing children with videos encouraging pornography and sex shops, TikTok changed its algorithm to stop recommending this type of content to young users in the future [2]. **Companies shall adopt proper default settings** (LR11) (e.g. deactivate profiling and geolocation by default) for their ecosystems to offer high-privacy and commercial-free platforms for children. Youtube Kids illustrates how this requirement can be implemented: to restrict access to adult content, Google enabled its SafeSearch filtering technology by default to users under 13 managed by its Google Family Link service [15].

Also, **companies shall promote parental controls and mediation in the platform** (LR12) by creating tools that enable age appropriate and transparent information about data protection to children and parents. An example of such tool is found in TikTok ecosystem, which offers a Family Pairing tool that allows parents to link their accounts to that of their child to manage the privacy settings [5]. Besides, **companies shall guarantee children's right to use, play and participate without data collection** (LR13), with features that are free from data processing. Although children must be offered the possibility to cease data collection, ecosystems from Big Techs such as Youtube Kids and TikTok do not provide this option. **Companies shall promote the right to disconnect from their platform** (LR14) by providing time restriction tools and avoiding features that encourage constant use. Google released tools that activate "take a break" and bedtime reminders by default for users under 17 [15].

3.3 Product and service provision

Respecting the CRC involves reduced risks in platform's products or services. Accordingly, **companies shall create a children's data protection impact assessments** (LR15) to mitigate the risks for children in the ecosystem. Since this an internal process or artefact, we could not identify related examples in the ecosystems that illustrate our requirements. However, we could infer that this is a neglected process, given the several threats caused to underage users by platforms such as TikTok, which was accused of promoting excessive risk-taking challenges, for example [4]. **Platforms shall avoid detrimental use of data** (LR16) to prevent persuasive design to extend engagement, marketing, and behavioural advertising. An example of concern with this requirements comes from Youtube Kids ecosystem: Google blocked ad targeting based on data like age, gender or interests for young teens and kids [15].

In addition, to **platforms shall offer age appropriate features** (LR17), i.e. age recommendations should not act as a validation for the detrimental use of children's data. Besides limiting platform features by age, ByteDance release an age-gating technology on TikTok to detect underage users for only presenting targeted ads to users who are 13+ [2,12]. In a similar fashion, **companies shall promote transparency, accessibility and legibility** (LR18), which can be done by providing all the information regarding the use of data in a simple, clear and constantly accessible form (e.g. translating such information into different languages and accessibility). TikTok Transparency Reports, which provide the community of users with details on guidelines enforcement, illustrates how this requirement can be implemented [21]. Finally, **companies shall avoid data sharing within the ecosystem** (LR19), as children's data is sensitive and should not be disclosed to partners. Google indeed shares children's data with third parties. However, data collection is limited to product requirements and parents can request to know what personal data third parties received [16].

4 Conclusion

The main contribution of this work was proposing a set of legal requirements that can act as a reference to evaluate platform ecosystem's diligence with children's privacy in terms of Children's Rights-by-Design. We invite researchers to extend this framework with additional guidance from UK's Information Commissioner's Office ("Age Appropriate Design Code") and Ireland's Data Protection Commission ("Children Front Centre: Fundamentals for a Child-Oriented Approach to Data Processing"), among others. A related work from Rafferty et al. [17] apply privacy requirements to Hello Barbie Privacy, revealing to what extent the toy's policy is compliant with it. However, their study focuses on smart toys instead of platforms. Pasquale et al. [14] investigated the mechanisms adopted by top social and communication apps to verify the age of their users, also offering recommendations for these providers to implement robust age verification tools. Despite addressing children's protection online, the authors centred their research on the verification of age limits.

In future work, we plan to

- Perform a mapping study on Computer Science, Law and Social Sciences literature to identify works approaching concerns about children's protection in platforms mainly formed by children, such as TikTok. This study must be complemented by a web search for news articles, reports and whitepapers about privacy and data protection on such platforms.
- Refine the structure of the list of legal requirements by (i) grouping them according to the main aspects they cover (e.g. data collection, data control by users, etc.), (ii) further specifying them for an adequate evaluation, presenting a list of fine-grained legal requirements, and (iii) prioritising the final set of requirements to determine the importance/impact of each one.
- Examine a selected group of platforms (e.g. TikTok, Youtube Kids. etc.) in terms of data use. Finally, we seek to present our findings to representatives of these platforms so that we obtain complementary views on platform's compliance with the legal requirements.

References

1. Assembly, U.G.: Convention on the rights of the child. United Nations, Treaty Series **1577**(3), 1–23 (1989)
2. Barry, R.: How tiktok serves up sex and drug videos to minors (Sep 2021), https://tinyurl.com/3ya2fd4b, access date: Oct 1, 2021
3. BBC: Tiktok sued for billions over use of children's data (Sep 2021), https://tinyurl.com/2p8s9a6t, access date: Oct 5, 2021
4. Chase, K.M.: How to talk to your kids about the devious licks school tiktok challenge (Sep 2021), https://tinyurl.com/yc7uc722, access date: Oct 1, 2021
5. Criddle, C.: Tiktok removes more than seven million suspected under-age accounts (Sep 2021), https://tinyurl.com/3sss73hh, access date: Oct 4, 2021
6. Dans, E.: Why has it taken four years for tiktok to finally move to protect its underage users? (Jan 2021), https://tinyurl.com/2e6j2ebf, access date: Oct 2, 2021
7. Frenkel, S., Mac, R., Isaac, M.: Instagram struggles with fears of losing its 'pipeline': Young users (Oct 2021), https://tinyurl.com/yrcsy876, access date: Oct 5, 2021
8. Google: Family link privacy guide for children teens, https://tinyurl.com/ypweyw8y, access date: Mar 1, 2022
9. Hartung, P.: The children's rights-by-design standard for data use by tech companies. UNICEF (2020)
10. Kavenna, J.: Surveillance capitalism is an assault on human autonomy (2019), https://tinyurl.com/4tp5y2vz, access date: Oct 3, 2021
11. Livingstone, S., Carr, J., Byrne, J.: Internet governance and children's rights (2016)
12. Lomas, N.: Eu to review tiktok's tos after child safety complaints (Sep 2021), https://tinyurl.com/mzyyja74, access date: Oct 3, 2021
13. Lomas, N.: Tiktok removes 500k+ accounts in italy after dpa order to block underage users (Sep 2021), https://tinyurl.com/mtp3cwes, access date: Oct 5, 2021
14. Pasquale, L., Zippo, P., Curley, C., O'Neill, B., Mongiello, M.: Digital age of consent and age verification: Can they protect children? IEEE Software (2020)
15. Perez, S.: Google to introduce increased protections for minors on its platform, including search, youtube and more (Aug 2021), https://tinyurl.com/e3v82sup, access date: Oct 5, 2021

16. Program, C.S.P.: Standard privacy report for google family link, https://tinyurl.com/jyunn3t4, access date: Jun 1, 2022
17. Rafferty, L., Fantinato, M., Hung, P.C.: Privacy requirements in toy computing. In: Mobile services for toy computing, pp. 141–173. Springer (2015)
18. Rebelo, M.E., Valença, G., Lins, F.: Power and privacy in software ecosystems: A study on data breach impact on tech giants. In: 27th REFSq. pp. 149–164 (2021)
19. Ridley, K.: Tiktok faces claim for billions in london child privacy lawsuit (Sep 2021), https://tinyurl.com/yckzhsy2, access date: Oct 3, 2021
20. Singer, N., Conger, K.: (Sep 2019), https://tinyurl.com/2p8akvxb, access date: August 10, 2021
21. TikTok: Transp. reports, https://tinyurl.com/4mdcss72, access date: Mar 1, 2022
22. Valença, G., Alves, C.: A theory of power in emerging software ecosystems formed by small-to-medium enterprises. J. of Systems and Software **134**, 76–104 (2017)