IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Digital Guardianship: Safeguarding Children In The Cyber Landscape

By Simran Bajaj & Mini Srivastava

Final Year student, Amity Law School, Amity University Noida, UP; Assistant Professor-II, Amity Law School, Amity University Noida, UP

Abstract

This paper delves into the intricate web of challenges that children encounter in the digital space, such as cyberbullying, exposure to inappropriate content, and privacy breaches. With the internet becoming an inseparable aspect of their lives, the necessity for robust digital guardianship is emphasized. We critically examine the Digital Personal Data Protection Act, 2023, in the context of protecting children's online privacy and personal data. Despite the Act's intent to safeguard minors, we argue that its implementation might be utopian due to vague definitions, lack of precise enforcement mechanisms, and the broad categorization of a 'child'. Furthermore, the paper discusses the contentious issue of defining a child in the digital era and suggests a more nuanced, age-graduated approach to consent and online participation. By scrutinizing the Act's stipulations and the broader societal and technological challenges, this research aims to shed light on the need for a forward-looking, adaptable legal framework that balances protection with the empowerment of children in navigating the digital world.

Keywords- Data Protection, Children, Privacy

I. Introduction

In today's digital age, safeguarding the well-being of children in online environments is of utmost importance due to the multitude of threats they face to their privacy. With the increasing presence of children on various online platforms, including social media and virtual spaces, they are vulnerable to risks such as cyberbullying, exposure to inappropriate content, and potential data exploitation.

The pervasive influence of the internet has significantly impacted children, particularly in more developed nations, where online communication has become an integral aspect of their daily lives from an early age. A substantial portion of children's time is now spent engaging in online activities. While this integration offers numerous benefits such as access to information, avenues for self-expression, heightened awareness, and enhanced social interaction, it also exposes children to well-documented dangers like exploitation and abuse by adults, cyberbullying, and excessive internet use.

One particularly concerning risk is the potential misuse or mishandling of children's personal information and online activities, emphasizing the critical necessity for robust regulations and technological safeguards to ensure their privacy. It's imperative to strike a delicate balance between facilitating exploration and shielding young users from potential harm.

However, policymaking responses to these challenges have often been reactive and disjointed. Frequently, policies are formulated without adequate consultation with children or a thorough assessment of their impact, thereby disregarding children's legal rights. While initiatives aimed at shielding children from online risks are commendable, they sometimes inadvertently impede children's access to the benefits of the digital realm, which they rightfully share with adults.

A more effective approach involves integrating digital literacy education with the principles of informed consent. This rights-based strategy seamlessly combines children's entitlement to protection with their freedom to utilize the internet.

Rooted in the United Nations Convention on the Rights of the Child (CRC), the concept of children's rights recognizes the inherent dignity and entitlement of every child to fundamental rights. With the digital landscape becoming an integral aspect of children's lives, these rights naturally extend to the online sphere, necessitating a robust legal framework for their protection. [1]

A study conducted in 2021 by the National Commission for Protection of Child Rights in India shed light on the prevalence of children's online engagement. It revealed that 30.2% of children aged 8-18 utilized smartphones or internet-connected devices for online learning. Additionally, children reported significant internet usage for accessing messaging apps, study materials, music, and games. Of concern, the study identified

[1] "Safeguarding Children's Rights In The Digital Age: Challenges And Opportunities," Legal Vidhiya, https://legalvidhiya.com/safeguarding-childrens-rights-in-the-digital-age-challenges-and-opportunities/#:~:text=In%20the%20digital%20age%2C%20children's,in%20this%20context%20as%20well (last visited Apr. 6, 2024).

that approximately 37.8% and 24.3% of 10-year-old children had Facebook and Instagram accounts, respectively. [2]

II. CHALLENGES FACED BY CHILDREN IN THE DIGITAL SPACE

In the rapidly evolving digital landscape, children face a myriad of challenges that can significantly impact their development and well-being. As they navigate through a vast online world, they are exposed to issues ranging from cyberbullying and privacy invasions to the detrimental effects of screen addiction and exposure to inappropriate content. These challenges not only threaten their mental and emotional health but also pose serious risks to their safety and privacy. Consequently, understanding and addressing these challenges is crucial for creating a safer and more nurturing digital environment for our youngest internet users.

Exploring the challenges faced by children in their digital presence unveils several concerns, such as:

1. Cyberbullying
2. Exposure to inappropriate content
3. Privacy breaches
4. Limited exposure to the physical world
5. Lack of Digital Literacy
6. Mental Health & Real-world Impact
7. Identity Theft

In a digital era marked by the increase of information and communication technology, these issues are on the rise, emphasizing the need for increased awareness and effective solutions.

1. ***Cyberbullying*** refers to the use of digital communication tools, such as social media, messaging apps, or online platforms, to harass, intimidate, or harm others. It can impact kids profoundly, causing emotional distress, anxiety, depression, and even leading to tragic outcomes like self-harm or suicide. The anonymity and widespread reach of cyberbullying exacerbates its effects, making it crucial to address and prevent in the context of children's online experiences. For instance, The ***Megan Meier case***[3] involved a 13-year-old girl who tragically took her own life after being cyberbullied through a fake online profile created by an adult neighbor's mother. The incident highlighted the devastating consequences of online harassment and underscored the need for increased awareness and legal measures to address cyberbullying.

[2] "Shepherding Children in the Digital Age," Times of India Blogs, https://timesofindia.indiatimes.com/blogs/voices/shepherding-children-in-the-digital-age/ (last visited Apr. 6, 2024).
[3] *Lauren Collins*, Friend Game-Behind the online hoax that led to a girl's suicide https://www.newyorker.com/magazine/2008/01/21/friend-game (last visited Apr. 6, 2024).

2. ***Exposure to inappropriate content*** poses a risk to children online, including explicit material or violent imagery. This can impact their mental and emotional well-being, making it crucial for parents and guardians to implement effective parental controls and monitoring measures to safeguard children's online experiences. In response to the criticism and concerns about children's exposure to inappropriate content, ***YouTube implemented significant changes to its algorithm***[4]. These modifications aimed to enhance content filtering and reduce the likelihood of harmful videos reaching young audiences. Additionally, YouTube introduced YouTube Kids, a dedicated platform with carefully curated and age-appropriate content, providing a safer online space for children to explore and enjoy digital content under the supervision of parents and guardians.

3. ***Privacy concerns*** for children in the digital realm are significant, with potential risks arising from the collection and misuse of their personal information. Children may unknowingly share sensitive data on social media platforms or through online interactions, making them vulnerable to privacy breaches, identity theft, and targeted advertising. Safeguarding children's privacy requires robust regulations, parental guidance, and age-appropriate online platforms with stringent privacy settings to ensure their digital experiences are secure and protected.

4. ***Excessive screen time*** and ***frequent use of social media*** can contribute to ***digital addiction*** among children, impacting their mental health. Prolonged exposure may lead to social isolation, disrupted sleep patterns, and increased vulnerability to cyberbullying. The curated nature of content on social platforms may also contribute to ***body image issues*** and ***a fear of missing out (FOMO),*** affecting children's self-esteem and mental well-being. Addressing these concerns requires promoting a balanced approach to digital engagement, fostering open communication, and enhancing digital literacy to help children navigate the online world responsibly. Creating awareness about the potential impact of excessive screen time on mental health is crucial for parents, educators, and society at large.

5. The ***lack of digital literacy*** among children significantly impacts their online experiences and well-being. With limited awareness of potential risks, children may unwittingly expose themselves to cyberbullying, inappropriate content, and interactions with online predators. The inability to critically evaluate information leaves them susceptible to misinformation, affecting their understanding of the digital landscape. Insufficient knowledge about online privacy can result in the unintentional sharing of personal details, while unhealthy media consumption habits may adversely affect their physical and

[4] "YouTube's Recent Algorithm Change Explains Why Your Feed Is Full of Children's Videos," The Verge, https://www.theverge.com/2019/8/1/20750054/youtube-algorithm-recommendation-kids-videos-cartoons-nursery-rhymes (last visited Apr. 6, 2024).

mental health. Moreover, a lack of understanding regarding the long-term consequences of online behavior can impact children's reputation and relationships. Addressing these challenges necessitates comprehensive digital literacy education, emphasizing the crucial role of schools and parents in equipping children with the skills needed for responsible and secure engagement in the digital world.

6. For children, prolonged exposure to screens, particularly in the context of the metaverse and extensive social media engagement, can have notable implications for their ***mental health and real-world impact***. The immersive nature of the metaverse and constant connectivity through social media may contribute to ***heightened stress, anxiety, and a distorted perception of reality***. Extended screen time can disrupt sleep patterns, an essential component of children's mental and physical well-being. Poor sleep quality may lead to changes in behavior, affecting their performance in school, relationships with peers and family, and overall daily routines. The potential consequences include difficulties in concentration, increased irritability, and challenges in managing emotions, all of which can significantly impact a child's psychological well-being and real-world functioning.

7. ***Identity theft*** concerning children's online presence poses a significant threat as youngsters often unknowingly share personal information, such as their names, birthdates, and school details, in the digital realm. This information can be exploited by identity thieves to create synthetic identities or ***attempt financial fraud, using a child's clean credit history***. The misuse of Social Security numbers is a particular concern, with potential long-term consequences for a child's future financial stability and creditworthiness. Identity theft in the context of children may also involve unauthorized access to their online accounts, leading to the compromise of personal information and the potential for cyberbullying or harassment. Parents play a crucial role in mitigating these risks by educating their children about online privacy, monitoring their online activities, and being vigilant against potential signs of identity theft. Additionally, online platforms need to enhance security measures to protect the sensitive information of underage users and prevent unauthorized access.

   Addressing the privacy concerns of children in the digital realm requires a multifaceted approach with several key solutions.

III. STATUS OF CHILDREN UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

A firmly established principle emphasizes the need for enhanced protection of children's privacy and personal information processing compared to the general data processing, given children's limited ability to fully grasp the implications of their actions. The Supreme Court, in declaring the Right to Privacy a fundamental right in 2017, acknowledged this perspective, stating *"children around the world create perpetual digital footprints on social network websites on a 24/7 basis as they learn their 'ABCs': Apple, Bluetooth, and Chat followed by Download, E-Mail, Facebook, Google, Hotmail, and Instagram. They should not be subjected to the consequences of their childish mistakes and naivety, their entire life. Privacy of children will require special protection not just in the context of the virtual world, but also the real world."*[5]

Under the Digital Personal Data Protection Act, 2023, children in India are given significant consideration to ensure their safety and privacy in the digital space. A "child" is defined as anyone under the age of 18, aligning with the broader understanding of minors. This act mandates that Data Fiduciaries, entities that process personal data, obtain consent from a parent or guardian before processing a child's data. Furthermore, it explicitly prohibits the processing of data that could harm a child's well-being, including any form of tracking or targeted advertising aimed at children. These provisions signify a robust stance towards protecting minors from the potential perils of digital data processing, underscoring the importance of safeguarding their digital footprint from exploitation and ensuring a safer online environment. The act also introduces severe penalties for non-compliance, with fines up to 200 crore rupees for failing to honor obligations related to children's personal data, highlighting the gravity with which children's data protection is regarded.

Section 9 of the DPDP Act 2023 reads as follows-

> *9. (1) The Data Fiduciary shall, before processing any personal data of a child or a person with disability who has a lawful guardian obtain verifiable consent of the parent of such child or the lawful guardian, as the case may be, in such manner as may be prescribed. Explanation. —For the purpose of this sub-section, the expression "consent of the parent" includes the consent of lawful guardian, wherever applicable.*
>
> *(2) A Data Fiduciary shall not undertake such processing of personal data that is likely to cause any detrimental effect on the well-being of a child.*
>
> *(3) A Data Fiduciary shall not undertake tracking or behavioural monitoring of children or targeted*

[5] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).

advertising directed at children.

(4) The provisions of sub-sections (1) and (3) shall not be applicable to processing of personal data of a child by such classes of Data Fiduciaries or for such purposes, and subject to such conditions, as may be prescribed.

(5) The Central Government may, if satisfied that a Data Fiduciary has ensured that its processing of personal data of children is done in a manner that is verifiably safe, notify for such processing by such Data Fiduciary the age above which that Data Fiduciary shall be exempt from the applicability of all or any of the obligations under sub-sections (1) and (3) in respect of processing by that Data Fiduciary as the notification may specify.

Despite the Digital Personal Data Protection Act, 2023's robust framework aimed at safeguarding children's privacy in the digital realm, certain gaps within the law remain evident, necessitating further refinement to enhance protections.

i. A Need To Change The Definition Of A Child

Determining the definition of a 'child' is a contentious issue in the contemporary digital environment. Although the United Nations Convention on the Rights of the Child (CRC) says in Article 1 that a child refers to every human being below the age of eighteen, unless the law applicable to the child establishes an earlier majority, setting the age limit at 18 may be impractical in today's context.

Treating all individuals under the age of 18 as a uniform and undifferentiated group appears excessive and overlooks the complexities of our contemporary reality. For example, requiring a 15-year-old teenager to obtain parental consent for activities like setting up a social media account or monitoring her menstrual health may not be practical or equitable. This is especially true considering that in many regions, topics such as menstruation and sexual health remain taboo despite efforts to address them. Additionally, there is a noticeable gender bias favoring the protection of girls over boys, even though boys often face more frequent online threats such as attempted account theft, financial information leaks, and unauthorized use of their personal data.

Simply put, it involves repeatedly seeking your parents' approval, not only when exploring one site but potentially each time you wish to visit a different one. This paints a picture of the internet browsing experience that teenagers might encounter under the existing provisions of the Act.

Reflecting on the 2022 iteration of the bill, it becomes evident that there is a pressing need to grant adolescents agency over different types of data at distinct ages. Such an approach is essential for upholding their fundamental rights to privacy and dignity as they navigate the digital landscape. Additionally, the current approach could potentially lead to gender-based discrimination. Considering societal norms, a distinction is

drawn between a boy and a girl seeking permission to create social media accounts, with girls likely facing more resistance.

Delving into the broader discourse surrounding parental consent, there is a notable emphasis on the significance of digital literacy. The observation is made that parents, in many instances, learn about internet usage from their children. This dynamic raises critical questions about parents' capacity to make informed decisions regarding their children's online activities. It challenges the assumption that parents possess comprehensive knowledge of which websites are suitable or unsuitable for their children. Consequently, this underlines the evolving nature of digital literacy within families and the necessity for a nuanced understanding when crafting regulations that govern children's online experiences.

From a global perspective- many nations distinguish between the age of consent in offline settings and the digital age of consent. For instance, in the European Union (EU), where the age of majority is generally set at 18 (except in Scotland), the General Data Protection Regulation (GDPR) designates the age of a child as 16, with member states having the option to lower it, provided it does not fall below 13. Consequently, countries like Belgium, Denmark, and Croatia have reduced the age of consent to 13. In the United States, the Children's Online Privacy Protection Act (COPPA) defines a child as an individual under 13.

For that matter in India, insights can be gleaned from various legislations within the country. For instance, in criminal law, individuals under the age of 12 are considered incapable of giving informed consent, while those between 12 and 18 years leave their maturity to the discretion of the court. Amendments to the Juvenile Justice Act also allow individuals aged 16 to 18 to be tried as adults for heinous crimes. Likewise, labor laws in the country differentiate between children (under 14 years) and adolescents (14 to 18), permitting adolescents to be employed in non-hazardous industries.

India's latest Digital Personal Data Protection (DPDP) Act restricts children's internet access by defining a child as an individual under eighteen years old. This mirrors the 2022 version, which faced criticism for treating all individuals under 18 uniformly, neglecting suggestions from experts. These experts recommended a ***graded approach***, differentiating between those aged 13 to 16 and those below 13. The experts emphasized the importance of acknowledging children's rights in the digital realm and the necessity for tailored regulations. However, the current legislation categorizes everyone from 0 to 17 years old under the broad label of "children," rather than adopting a more nuanced approach.

A graded approach is advocated for several reasons, particularly in the context of regulations related to age categories, such as those concerning internet access and data protection for children:

- **Developmental Differences**: Children undergo significant developmental changes during adolescence. A graded approach recognizes that the needs, capacities, and understanding of online risks and responsibilities vary across different age groups.

- **Cognitive and Emotional Maturity:** Younger children, typically below 13, may have different cognitive and emotional capacities compared to teenagers aged 13 to 16. Tailored regulations can acknowledge these differences and provide age-appropriate safeguards.
- **Educational Considerations:** Older adolescents may be more equipped to handle certain online activities responsibly. A graded approach allows regulations to align with educational needs, ensuring that young individuals can benefit from online resources while being protected from potential risks.
- **Informed Decision-Making:** Adolescents aged 13 to 16 may be more capable of making informed decisions about their online activities. Tailored regulations empower them with a level of autonomy while still providing necessary protections.
- **Respect for Autonomy:** Recognizing age-based differences respects the growing autonomy of adolescents and allows for a balanced approach that fosters independence while maintaining a focus on their protection.

The bottom line is that adopting a graded approach in addressing various aspects related to children offline should also be mirrored in the online realm.

Children, particularly those who are digitally savvy, may find ways to bypass imposed restrictions. Therefore, the emphasis should shift towards equipping minors with the knowledge to safeguard themselves from potential risks in the digital realm. This involves:

- Prioritizing empowering minors with knowledge to navigate digital spaces and protect themselves.
- Implementing regulations requiring tech companies collecting children's data to follow best practices and seek age-appropriate consent.
- Conducting empirical research in India to establish well-reasoned categories for children based on varying levels of maturity.
- Introducing different categories for consent requirements, considering age-appropriate information sharing.

ii. How Can Websites Secure Parental/Guardian Consent?

Both the Act and the 2022 bill mandate online platforms to obtain ***"verifiable parental consent"*** before processing a child's data. This could involve various methods, ranging from facial recognition software to the submission of official documents like Aadhaar, or a combination of these. However, the requirement for verifiable consent presents its own set of challenges.

It's essential to recognize that implementing age verification for everyone, regardless of whether they are minors or adults, would result in an excessive level of public surveillance. Similar concerns were raised in California's Age-Appropriate Design Code, where experts said that ***age verification requirements undermine online anonymity***, posing a threat to the freedom of expression for activists, whistleblowers, journalists, and others.

In view of the intricacies of obtaining verifiable parental consent, all websites or applications utilized by individuals in India will need to undergo age verification and obtain parental consent, as delineated in section 9(1). Companies or categories seeking an exemption must be officially approved (whitelisted) by the Indian government, in accordance with the stipulations in sections 9(4) and 9(5).

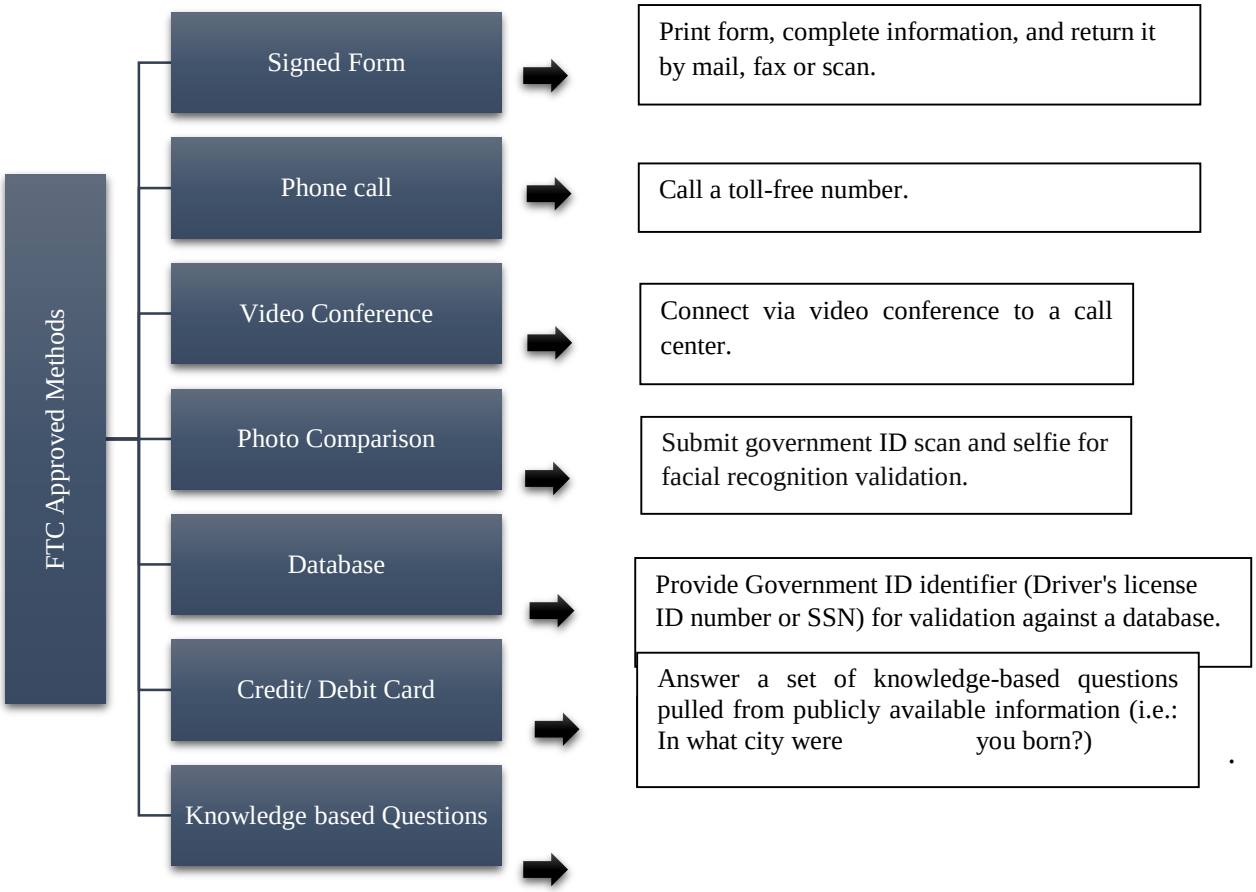
Traditional parental consent is a concept applicable when offering contractual services to children who are legally unable to enter into contracts. Unlike the traditional approach, which assumes easy verification of parental status in physical interactions, the challenge in the online domain. The online domain distinguishes itself by being provided remotely, where the service provider and the customer are not physically present together. In response to this, modern privacy laws governing ISS in many countries emphasize the need for verifiable parental consent. The Digital Personal Data Protection Act, 2023 (DPDPA) similarly mandates entities processing children's personal data to obtain verifiable parental consent. However***, the Act does not specify methods for verifying parental consent***. Thus, the Act may not effectively address the complexities associated with the use of advanced technology for verifying parental consent.

a. What Others Are Doing?

In jurisdictions where privacy laws are in effect, various models regulate the procedures for validating parental consent. In the United States, the processing of children's personal data by websites is governed by the ***Children's Online Privacy Protection Act ("COPPA")***. This legislation stipulates the necessity of obtaining verifiable parental consent prior to the processing of children's personal data. The ***Federal Trade Commission ("FTC")*** is entrusted with outlining the ***methods for securing verifiable parental consent.*** The FTC has furnished a non-exhaustive compilation of acceptable technologies that websites can employ to obtain verifiable parental consent. Other than FTC approved technologies, innovative technologies can be proposed to the FTC for evaluation, and upon approval, they become recognized as valid means of obtaining verifiable parental consent. ISS is obligated to incorporate at least one of the approved methods to showcase adherence to the verifiable parental consent requirement.

In contrast, the European Union does not furnish a catalog of sanctioned methods; instead, it delineates factors that can influence the selection of a method. These considerations encompass the nature of the personal data, the purposes of processing, and the potential risks associated with the process. ISS has the flexibility to choose a method that effectively addresses these influencing factors.

b. Methods of Verifiable Consent (FTC Approved)



c. How It Works

There is currently no comprehensive digital identity system for the internet, making it challenging to easily determine whether a website user is a child or an adult, and to ascertain if the individual providing consent is the parent of a child user. In response to this gap, various techniques and technologies related to Verified Parental Consent (VPC) have emerged, shaping the current landscape of VPC practices.

Numerous websites fall under the category of "general audience" services, meaning they are not specifically designed for children, and the operators have no explicit knowledge of children using the site. COPPA generally does not mandate that general audience services deduce users' ages, but it does require these sites to take action when notified by children, parents, or others about a specific child using the service. COPPA outlines specific obligations for covered operators, such as those of commercial online services directed to children under 13 or those with actual knowledge that a child under 13 uses the service. These obligations include implementing measures to safeguard the privacy of personal information collected from children, such as posting a privacy policy detailing how the operator manages children's personal information, providing parents with direct notice of information practices, obtaining verifiable consent from parents before collecting, using, or disclosing their children's personal information, and honoring parents' subsequent requests to review or delete data collected about their children.

d. The Zero-Age Screening System

The crucial question to address is: ***how can operators determine when it is necessary to obtain Verified Parental Consent (VPC) for a specific user?*** Operators face a challenge as they cannot compel children to ask their parents for permission if they are unaware that a child is using their platform, and therefore, cannot prompt the child to seek consent. To identify whether a user needs VPC—preceding the formal VPC process—websites and online services, particularly those not primarily catering to children under 13, often employ an age screening system, commonly referred to as an "age gate." Some general audience websites also use age screening systems to restrict access for children under 13. Social media platforms, for instance, frequently employ these systems to prevent underage users, and websites advertising age-restricted products like alcohol use them to restrict access for individuals under 18 or 21.[7]

In accordance with FTC guidelines, age screening systems must be "neutral." Users are prompted to provide their age by entering their month and year of birth, as opposed to a simple inquiry about whether they are 13 or older. This approach aims to prevent child users from realizing that they need to input a specific birth year, regardless of their actual age, to gain access to the service. The FTC prohibits websites targeting children from implementing age screening systems to prevent users under 13 from accessing their service because if the service is directed at children, it must adhere to the requirements for providing access to children under 13. VPC is mandated for the collection of Personally Identifiable Information (PII) on sites directed to children, regardless of the presence of an age screen.

Following the age screening process, operators are required to provide direct parental notice and potentially obtain Verified Parental Consent (VPC), which serves as the digital "permission to play." The Children's Online Privacy Protection Act (COPPA) specifies the instances in which VPC is necessary. COPPA obligations, including VPC, come into play when an operator or a third party with actual knowledge collects, uses, or discloses a child's personal information.

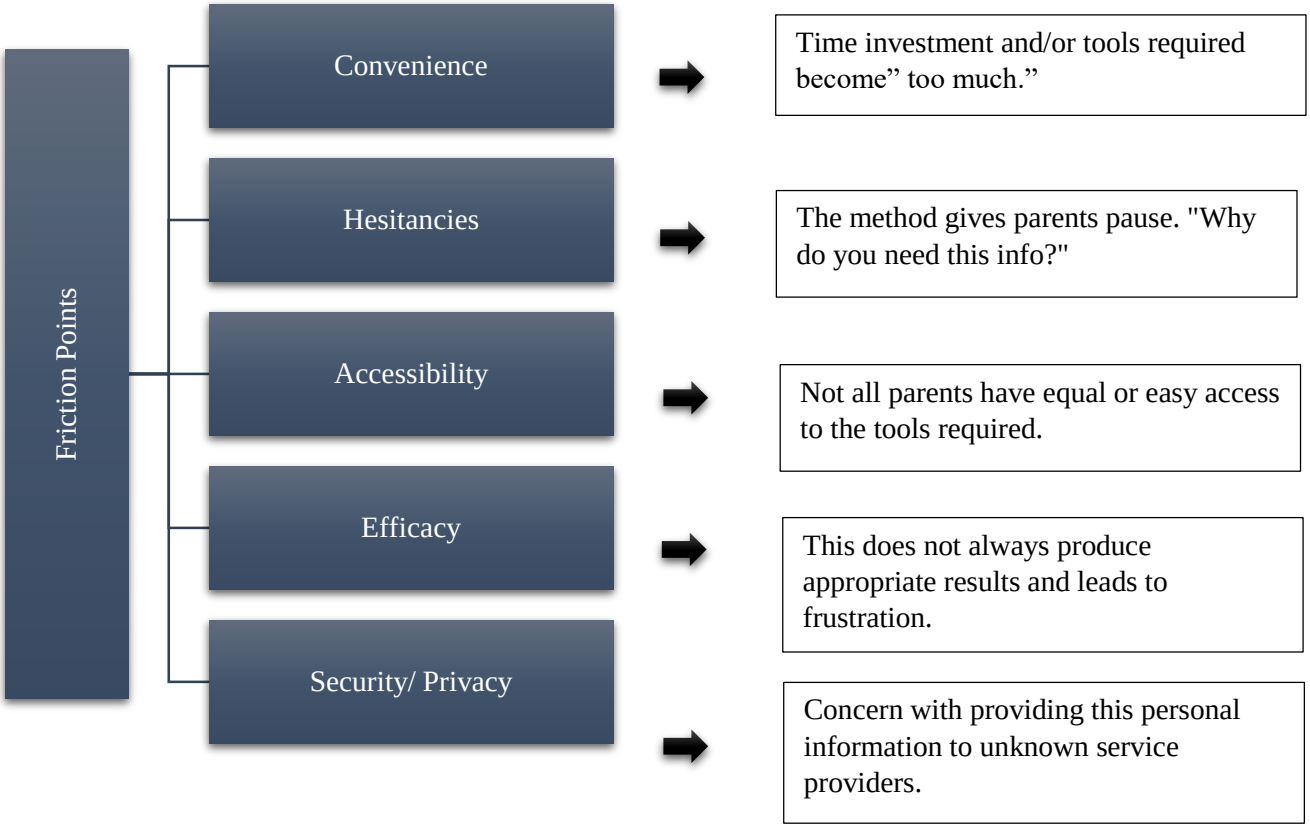
The collection of a child's personal information can take various forms, such as-

- requesting, prompting, or encouraging a child to submit personal information online;
- allowing a child to make personal information publicly available, for instance, through access to a public chat forum without making reasonable efforts to redact or delete the information before posting; or

[6] Future of Privacy Forum, FPF VPC White Paper (2023), https://fpf.org/wp-content/uploads/2023/06/FPF-VPC-White-Paper-06-02-23-final2.pdf (last visited Apr. 6, 2024).
[7] Future of Privacy Forum, FPF VPC White Paper (2023), https://fpf.org/wp-content/uploads/2023/06/FPF-VPC-White-Paper-06-02-23-final2.pdf (last visited Apr. 6, 2024).

- passively tracking a child online, including the collection of persistent identifiers, such as allowing third-party platforms to gather device identifiers for ad-targeting on an online site or service primarily directed to children. If any of these circumstances are present, the requirement for VPC arises.

e. The Friction Points In Implementing Ftc Approved Methods Of Verified Parental Consent



In this situation, there are two potential outcomes. Firstly, if the parent grants consent, the child will be able to access online content. Conversely, if the child provides false information about their age, they may potentially gain access to content that is not suitable for their age group. Additionally, if the parent withholds consent, the child will be restricted from participating in the online experience.

f. India's Take On It

1. Two methods for age verification are proposed:
    - ***Aadhaar-Based Authentication:*** Parents can add their children's Aadhaar details to the DigiLocker app. Platforms can then verify a user's age by pinging the app without revealing Aadhaar details.

- ***Electronic Token System:*** The industry may create a consent manager that tokenizes a user's government ID into an encrypted format, sharing only age and name parameters with the platform. This method requires government approval.

2. Some entities, like healthcare and educational institutions, may be exempted from obtaining verifiable parental consent and age-gating requirements. Exemptions could be granted on a restricted basis, depending on the specific purpose for which the entities need to process a child's data.

3. Entities are required to notify users about a data breach as soon as they become aware of it. The notification process involves two stages:
    - First, users are alerted about the nature and extent of the breach.
    - Second, users must be notified within 72 hours about additional details related to the breach.

4. Another key proposal of the rules will be to require government institutions to issue a notice to citizens whenever they are using their personal data for offering welfare services and subsidies, or for other similar activities.

iii. Protecting Children From Behavioral Tracking

The legislation under section 9(3) prohibits websites from engaging in the tracking or monitoring of children's behavior. For instance, imagine that you, as an adult, searched for a specific video game, and later, ads for that game started appearing on your social media accounts. If you were a child, the legislation would prevent websites from targeting you with such ads.

But the question is, *is behavioral tracking really a bad thing?*

Some websites, particularly those designed for educational purposes, may enhance their functionality through user tracking. Take, for instance, platforms providing adaptive assessments and periodic online evaluations for educational competitions; they could optimize students' learning experiences by tailoring tests to individual needs. Restricting websites from tracking such data, as proposed by the bill, might inadvertently dissuade companies from developing online services tailored for children.

To address this concern, the legislation includes provisions for exemptions on specific websites. It stipulates that if the central government deems certain online platforms to be handling data in a "***demonstrably secure manner***," they may be excused from the requirement to obtain parental consent and may also be permitted to engage in tracking children. Additionally, the government retains the authority to authorize the processing of children's data and behavioral monitoring for purposes that are yet to be specified.

Conclusion

The DPDP Act of 2023 lacks a forward-thinking approach as it overlooks the challenges arising in the digital realm, especially considering the continuous expansion of information and communication technology (ICT). A notable concern is the legislation's failure to address issues emerging in the metaverse, where crimes can inflict enduring mental impacts on users despite the absence of physical loss or injury.

In addressing the nuances of the digital landscape, the Digital Personal Data Protection Act, 2023, marks a significant stride towards safeguarding the privacy and security of children online. However, our analysis reveals critical gaps and areas for improvement within the act. The overarching challenge lies in reconciling the need for protective measures with the acknowledgment of children's evolving capabilities and rights in the digital domain. The act's current stipulations, while rooted in the intent to protect, may inadvertently stifle the autonomy and developmental needs of minors, particularly as they navigate the complexities of the internet.

The nuanced nature of digital interaction necessitates a dynamic approach to consent and participation, reflecting the diverse maturity levels among minors. Furthermore, the practical challenges of implementing verifiable parental consent highlight the need for innovative solutions that balance safety with usability, ensuring that protective measures do not become barriers to access.

Recommendations[8]

As we delve into the complexities of safeguarding children in the digital age, it becomes imperative to approach this challenge with a multifaceted and dynamic strategy. Recognizing the rapid evolution of digital landscapes and the diverse needs of minors navigating these spaces, our recommendations aim to bridge the gaps identified in the Digital Personal Data Protection Act, 2023. These proposals are designed not only to enhance the protection mechanisms for minors but also to empower them as active, informed participants in the digital realm. From revising the legal definition of a child to fostering a culture of digital literacy and public-private collaboration, these recommendations underscore the need for a holistic, adaptable approach to digital guardianship.[9]

1. **Revise the Definition of a Child**: Adopt a more nuanced, developmentally informed approach to defining 'child' within the legislation, recognizing varying levels of maturity and autonomy. This could involve establishing graded consent mechanisms to accommodate different age groups and competencies.

[8] The World Bank's reports on Digital Development: The World Bank, Digital Development, https://www.worldbank.org/en/topic/digitaldevelopment (last visited Apr. 6, 2024).
[9] United Nations Children's Fund (UNICEF): United Nations Children's Fund, https://www.unicef.org/ (last visited Apr. 6, 2024).

2. **Streamline Parental/Guardian Consent**: Develop standardized, secure, and user-friendly methods for obtaining verifiable parental or guardian consent. This could include leveraging existing digital ID systems or creating new digital platforms specifically designed for this purpose.

3. **Enhance Digital Literacy**: Implement comprehensive digital literacy programs for both children and parents, focusing on safe and responsible internet use, privacy protection, and awareness of digital rights. These programs should be integrated into school curricula and accessible through public campaigns.

4. **Promote Public-Private Collaboration**: Encourage collaboration between the government, technology companies, educational institutions, and civil society to develop innovative solutions for protecting children online. This could include creating age-appropriate digital environments and improving content moderation practices.

5. **Regularly Review and Update Legislation**: Establish mechanisms for the regular review and update of digital privacy laws to ensure they remain relevant in the face of rapidly evolving digital technologies and societal norms. This should involve input from a wide range of stakeholders, including the children themselves.[10]

By addressing these recommendations, India can move towards a more balanced and effective legal framework that not only protects children in the digital realm but also empowers them to navigate the online world safely and confidently.

References

1. "Safeguarding Children's Rights In The Digital Age: Challenges And Opportunities," Legal Vidhiya, https://legalvidhiya.com/safeguarding-childrens-rights-in-the-digital-age-challenges-and-opportunities/#:~:text=In%20the%20digital%20age%2C%20children's,in%20this%20context%20as%20well (last visited Apr. 6, 2024).

2. "Shepherding Children in the Digital Age," Times of India Blogs, https://timesofindia.indiatimes.com/blogs/voices/shepherding-children-in-the-digital-age/ (last visited Apr. 6, 2024).

3. *Lauren Collins*, Friend Game-Behind the online hoax that led to a girl's suicide https://www.newyorker.com/magazine/2008/01/21/friend-game (last visited Apr. 6, 2024).
4. "YouTube's Recent Algorithm Change Explains Why Your Feed Is Full of Children's Videos," The Verge, https://www.theverge.com/2019/8/1/20750054/youtube-algorithm-recommendation-kids-videos-cartoons-nursery-rhymes (last visited Apr. 6, 2024).

5. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).

[10] India's Ministry of Electronics & Information Technology: Ministry of Electronics & Information Technology, Government of India, https://www.meity.gov.in/ (last visited Apr. 6, 2024).

6. Future of Privacy Forum, FPF VPC White Paper (2023), https://fpf.org/wp-content/uploads/2023/06/FPF-VPC-White-Paper-06-02-23-final2.pdf (last visited Apr. 6, 2024).

7. Future of Privacy Forum, FPF VPC White Paper (2023), https://fpf.org/wp-content/uploads/2023/06/FPF-VPC-White-Paper-06-02-23-final2.pdf (last visited Apr. 6, 2024).

8. The World Bank's reports on Digital Development: The World Bank, Digital Development, https://www.worldbank.org/en/topic/digitaldevelopment (last visited Apr. 6, 2024).

9. United Nations Children's Fund (UNICEF): United Nations Children's Fund, https://www.unicef.org/ (last visited Apr. 6, 2024).