SAFEGUARDING CHILDREN'S DIGITAL FOOTPRINTS: A STUDY OF DATA PRIVACY LAWS FOR MINORS – INDIA AND U.S.

Dr. Priya J Shah, Jitendra Chauhan College of Law

ABSTRACT

Today, as children wind seamlessly into the surroundings around them in the elevated cyberspace globe, protecting their personal data becomes increasingly necessary. This paper discusses emerging data privacy laws for minors based on India's and the United States' contrasting legal frameworks on children's digital footprints. The point, however, is that while in the United States the chief regulation on children under thirteen is the Children's Online Privacy Protection Act (COPPA), here at home the regulatory milieu comprises the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, as well as the pending Personal Data Protection Bill, which promises to provide further stringent protection to children's online privacy. The nature and specific scope of the two-siloed regulations will be analyzed in terms of their effectiveness, enforcement, and alignment with global best practices. It observes issues such as parental consent, data retention, online advertising, as well as children's rights to control personal information, as treated in laws of the respective countries. Through the analysis of legal provisions in India and the U.S., the paper further points out challenges and gaps in current regulations and opportunities for strengthening children's rights in data protection. It also analyzes the impact of such laws on the behavioral changes of corporations and consumer trust besides the broad societal consequences of children's data privacy in an increasingly digitized landscape. Moreover, he recommended measures that could be taken for the improvement of safeguarding minors from digital data thereby providing lessons from both legal systems to develop a more robust and harmonized global approach to online privacy protection of children.

The study thus hopes to deepen the melting pot of arguments produced regarding technology, privacy, and child welfare while giving insight into the solutions found by both countries to the data privacy dilemmas that minors face in an increasingly digital environment.

Keywords: Data Privacy, Children's Digital Footprints, Minors, COPPA, Online Privacy

Introduction:

It is an alarming situation as children today are more exposed to the online world, especially social networks where there are educational technology applications where vast amounts of personal data will be stored. This has made child digital privacy a significant concern for policymakers, technology companies, and parents in the current scenario. There are minors' data privacy laws that prevent and protect their data from being misused and act as a buffer against violation or breach of privacy or exploitation within their personal life. However, these laws differ so much from one nation to another, leaving lopsided distribution of treatment of children's data worldwide.

The objective of this paper is to examine data privacy laws regarding minors in the two pioneering major jurisdictions, namely India and the United States. This comparative study will examine data privacy laws concerning minors in India and the United States by focusing on an analysis of the legal frameworks of both countries regarding children's online privacy and how the laws of each country define minors, consent, data retention, and disallowance of online advertisements targeting children. The main research question making the backbone of this paper is: "How do the data privacy laws for minors in India and the United States differ, and what are the implications of these differences for the protection of children's digital rights and the responsibilities of corporations?". Several reasons make this study important. It adds to the growing debate over children's data protection, an increasingly relevant topic, as children use digital environments at earlier ages. The paper compares regulatory frameworks in India and the U.S, shedding light on the effectiveness of existing laws and strengths, weaknesses, and areas for improvement. Knowing how different countries approach the matter of children's privacy in the digital world is important for all global efforts at protecting children rights in the digital realm, as the very nature of the internet transcends borders.

In addition, the study examines the implications of these laws on behavior and outcomes in the real world. This research analyzes whether businesses within these jurisdictions could comply with data privacy regulations such that children's personal data is protected while innovating effectively to engage users. Finally, this paper would also provide recommendations on strengthening the data privacy protection of children in India and the U.S. Such recommendations would hopefully inform policymakers, regulators, and advocates working toward creating a safer digital environment for minors across the globe. Through this analysis,

the report emphasizes the need for harmonization in children's data privacy beyond the barriers of geographical borders in lieu of shifting technological landscapes.

Data Privacy Laws for Children in India

India currently uses a combination of general information technology regulations with proposed data protection legislation for safeguarding a child's digital data. However, there is no dedicated statute specifically dealing with children's online privacy. The strongest existing legal instrument is the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, underSection43A of the Information Technology Act, 2000[1]. These rules require entities to take reasonable security practices when dealing with sensitive personal data, which by implication includes children's data, but do not provide specific provisions for minors.

Among the very few protections, parental or guardian consent is required for the collection of sensitive personal data from persons considered minors. However, the Rules do not define children nor set an age of digital consent, thereby creating a legally ambiguous situation about enforcement of such consent. Furthermore, with newer techniques of data collection and behavioral profiling all around, the 2011 Rules are considered obsolete. The Personal Data Protection Bill, 2019, provided a more progressive framework with a rights-based approach to data protection and a whole chapter on children's data. Under the PDPB, a child is defined as anybody under the age of 18 years, and data fiduciaries shall take verifiable consent of the parent or guardian of such children for processing any personal data of the child[2]. It also proposed to prohibit data fiduciaries to be considered "guardian data fiduciaries" in case they operate websites or services that are likely to be accessed by children from engaging in profiling, tracking, targeted advertising, or any practice causing significant harm to children[3].

Another major introduction in the PDPB is the Right to be Forgotten, whereby data principals, including minors, may request for personal data to be deleted under circumstances where the data is no longer necessary or where consent has been withdrawn[4]. If these provisions come into force, children and their parents or guardians would be given more power to determine

[1] Information Technology Act, 2000, § 43A; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[2] Personal Data Protection Bill, 2019, Chapter IV, Clause 16
[3] Ibid., Clause 16(3) and 16(4).
[4] Personal Data Protection Bill, 2019, Clause 20 – Right to be Forgotten.

how long a digital platform can retain their personal data and how it can then be used. Summed up, the Indian legal setup, which is still growing, has treated children's data privacy with increasing importance, but some significant impediments include practical enforcement, institutional preparedness, and digital literacy. Legislative intent should definitely be supported by a strong regulatory infrastructure, stakeholder awareness programs, and harmonization with international data protection standards for an actual protective environment to come into being. Despite these legislative strides, India faces various challenges in enforcement and implementation. Unlike the United States, which has a dedicated body known as the Federal Trade Commission (FTC) that works solely on children's digital privacy issues, India does not yet have an independent regulatory authority. On the other hand, public awareness of children's digital rights is at its lowest, especially among parents in rural and semi-urban areas. The lag of digital literacy among children, parents, and teachers weakens the effectiveness of even the strongest legal protections.

Summing up, this somewhat changing legal scenario of India manifests growing realization about the importance of children's data privacy; however, there still exist certain challenges in respect of enforcement strategies, and above all, readiness of institutions, digital education, et cetera. To ensure effective protection, the intent of the legislation, along with law enforcers' capacity building, stakeholder awareness programs, and global data protection harmonization, need to be addressed simultaneously.

Children’s Data Privacy and Exposure to Inappropriate Content on OTT Platforms in India.

Increased usage of OTT platforms by minors in India presents a new focal point in the ongoing discussion regarding child data privacy protection. Unlike films, TV serials, etc., being the ever-growing range of exclusive content from India in varied languages, these platforms carry several types of shows. Children manipulate age fields during registration on these platforms and get unrestricted access to content which is highly inappropriate and can be a risk psychologically, besides creating a danger to their digital privacy.

Currently, the primary legislation governing content regulation in India is the Cable Television Networks (Regulation) Act, 1995. This statute does regulate televised content by imposing guidelines concerning age-appropriate programs but does not extend these guidelines to digital streaming services such as OTT platforms, thus creating a serious legal void in the online

ecosystem. To address this lacuna, the Ministry of Information and Broadcasting (MIB) promulgated the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which contain self-regulatory provisions for OTT content and categorize programs on age-based ratings: **U (Universal), U/A 7+, U/A 13+, U/A 16+, and A (Adult)[5]. The guidelines encourage platform sides to instate parental controls and strong-age verification systems, especially with respect to adult-rated content. But age-verification systems today revolve around users declaring their age, which is the easiest thing to bypass. A child could simply input a false birth date or, in the worst-case scenario, just use an already-existing family account, granting them a free walk-through to any content meant for a particular age group. From this perspective, it hardly even sets up a fight for the enforcement of content regulations, but it further raises grave data privacy issues, as the child-user's browsing data and preferences are tracked and monetized without their informed consent.

OTT, being a digital service, is obliged under the Personal Data Protection Bill, 2019 (PDPB)—now converted into the Digital Personal Data Protection Act (DPDPA), 2023—to publish verifiable mechanisms of parental consent whenever they intend to process the personal data of anyone under 18[6]. A further consequence could be OTT platforms being classified "guardian data fiduciaries," thereby putting them under tougher restrictions for profiling, tracking, targeted advertising, and content recommendations of minors[7]. Until these two critical issues remain unsolved, however, bit by bit, the second layer of child protection and data privacy will remain an aspiration rather than a possibility. First, there exists an absence of stringent enforcement of these norms. They remain largely self-regulatory guidelines, with no centralized authority mandated and empowered to audit the implementation of age filters or parental controls. Secondly, attributability for violations remains in the grey. Whenever children are exposed to inappropriate content, or when clustered for advertising, responsibility lies in a murky dominion, sometimes with the platforms, sometimes with the parents, and sometimes with regulators. Moreover, the constitutional secured right to freedom of speech within the confines of reasonable restrictions, in other words, justifiability, is said to extend to operating age controls, with the question being whether age constraints stand in the way of reasonable restrictions. However, these supposed restrictions, either on one platform, are

[5] Ministry of Information and Broadcasting (2021). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*.
[6] Digital Personal Data Protection Act, 2023, Sec. 9 – Processing of personal data of children.
[7] Personal Data Protection Bill, 2019, Clause 16(4) – Obligations of guardian data fiduciaries.

absent on other platforms, or evade technical circumvention. This situation is exacerbated by the low digital literacy levels among Indian parents, many of whom are unaware of these content filters or how to activate them. Therefore, the regulation of OTT content must be buttressed with campaigns for digital literacy and parental awareness, equipping families to shield their children from such content and privacy risks.

To conclude, while India has made certain strides in moving toward regulating OTT content and protecting children's data privacy, implementation is still the Achilles' heel. Unless and until there is a foolproof verification method, enforcement is proactive, and through awareness, the users are enabled, the protection of children against adult content and data exploitation in the OTT arena in India shall always be the proverbial dream rather than reality.

United States – Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act[8] (COPPA), passed in 1998 and enforced by the Federal Trade Commission, serves as the primary legislation regarding the protection of children's online data in the United States. It extends to websites, mobile applications, and any other online services directed at children below 13 years of age or which knowingly collect personal information from a child belonging to this age group[9]. While COPPA does not provide any protection for adolescents aged 13 to 17, it is sometimes regarded as the benchmark framework for protecting children's digital privacy.

COPPA is designed to empower parents so that they can control what information is gathered on their young children online. It sets very strict standards for those bodies that deal with children's data and also provides for civil penalties where there are violations thereof.

The Children's Online Privacy Protection Act (COPPA) incorporates several provisions intended to ensure digital safety for children under 13. A primary provision is that Universal Parental Consent requires sites or online services collecting personal information from children aged 12 or below to seek clear approval from a parent or guardian before collecting, using, or disclosing such information[10]. Furthermore, the Act requires a platform to provide a privacy notice that is plainly written, easy to find, and describes its data practices so that the parents

[8] Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277
[9] 16 CFR 312.3
[10] Children's Online Privacy Protection Act (COPPA), 15 U.S.C. Sec. 6501–6506.

may be informed of how their child's data is being treated. The Act ensures that parents retain much control concerning information about their children online, allowing them to view, delete, or forbid further collection of their child's information. Other major principles under COPPA provide for data minimization; this means that sites can only collect data deemed necessary to provide a service or feature requested by the child. Finally, profiling and behavioral advertising are restricted. In essence, it refrains from targeting marketers who would exploit children's data for commercial purposes. These provisions collectively seek to lessen the chances of exploitation and ensure a safe, private, and age-appropriate online space for children. The Children's Online Privacy Protection Act, passed in 1998 and enforced by the Federal Trade Commission, is the chief statute governing the protection of children's online data in the United States. This act considers any sort of website, mobile application, or any other online service directed to children below 13 years of age or which knowingly collects personal information from a child belonging to said age. Even though COPPA offers no protection to adolescents ranging from 13 to 17 years, it is often considered the parent framework of digital privacy protection.

The act allows parents to exercise some level of control as to what information is gathered about their children on the Internet. It places very stringent requirements upon entities dealing with information regarding children, and it provides for civil penalties when violations are found.

Recommendation

Given the massive exposure to online platforms these days, and the digital ecosystem evolving, there is an urgent need to strengthen data privacy protection granted to minors. The lines of recommendations flowing toward enhanced protection of children's digital footprints are drawn from an analysis of legal regimes, enforcement challenges, and loopholes therein:

1. Harmonization of Age Thresholds for Consent

India and the United States differ on the notion of a "child" under data protection law. Whereas India goes to the extent of protecting anyone under 18, COPPA does so only for those under 13, thereby calling for harmonization of age thresholds at the international level to avoid any regulatory inconsistencies and to make sure that adolescents (13 to 17) are not excluded from

any privacy protection, especially since the highest percentage of internet use is that of teenagers.

2. Strengthening Age Verification Mechanisms

Self-declaration of age is not a prevention measure to keep a minor accessing inappropriate content or protective against data protection. Both jurisdictions should provide for strict-age verification tools that respect privacy and could be based on AI or digital ID systems, or parental Consent tokenized in some fashion. Furthermore, the regulatory bodies should issue explicit technical standards that apply to the methodologies of verification.

3. Privacy by Design: Legal Requirement

Child-facilitating platforms should have the legal requirement to be designed with privacy by design and privacy by default principles. These include profiling, tracking, location sharing, and targeted advertising path, all should be disabled unless there is a clear, informed consent from a parent.

4. Unified Enforcement Mechanisms and Penalties

India must set up a specialized regulatory agency or body (such as a Children's Data Protection Division under the Data Protection Board) for uniform enforcement and to address violations relating to children. The U.S. may strengthen interagency cooperation among various state agencies to also oversee compliance by EdTech and OTT platforms.

5. Mandatory DPIAs

Both countries must have child-specific Data Protection Impact Assessments done by platforms processing children's data. These inspections should be presented to the regulator and partly made public, thereby assuring transparency in data practices and risk management.

6. Digital Literacy and Awareness Creation

Legal provisions alone are insufficient without accompanying campaigns for public awareness. So, governments in collaboration with civil society and educational institutions should conduct

nationwide programs for the education of parents and children about digital privacy rights, safe browsing, and reporting mechanisms.

7. Regulation of OTT and Content Platforms

The OTT industry needs to be brought under a comprehensive statutory content and privacy regime, especially for children. This legislation should require content filters, default privacy settings for child profiles, and real-time enforcement mechanisms to flag inappropriate content or data misuse.

8. Cooperation Globally on Cross-Border Data Protection

Being that digital content and services transcend national boundaries, India and the U.S. should cooperate bilaterally and multilaterally to create interoperable privacy frameworks for children, share best practices, harmonize definitions, and guarantee reciprocal enforcement of child protection norms.

Conclusion

In an era when digital engagement begins early in childhood and the digital platforms in one way or the other structure the social, educational, and recreational experiences of a child, the protection of the child's digital footprint must stand as a legal imperative and a social responsibility. Hence, it was demonstrated by this research that while both India and the United States have a framework that aims to safeguard children's data, glaring gaps in scope, enforcement, and adaptation remain.

In conceptual terms, India, with a broad definition of a child including everyone below 18 years of age, hopes to offer a wider protective umbrella. Laws such as the IT Rules or the fledgling Digital Personal Data Protection Act in India however, face many challenges in implementation with respect to institutional capacity, public awareness, and platform accountability. The United States, in turn, is perhaps better in enforcement under COPPA and some nascent state-level attempts but not enough to protect adequately many adolescents (13–17) and falls behind in the very nature of the digital reality, which is fast changing. Every day, there is an influx of data being amassed by OTT platforms and social media sites on the one hand and edtech companies on the other-from minors, almost always without informed consent or adequate mechanisms for protection. This ever-growing risk of gross misuse of data, profiling of

individuals, and exposure to harmful content cannot be furthered by uncoordinated self-regulation, cheap and unreliable age verification tools, or arbitrary filtering practices.

Hence it is imperative that countries and, indeed, the international community move away from piecemeal attempts toward a harmonized, child-righteous framework of digital privacy. Stronger legislation and proactive enforcement must be introduced alongside a technical standard, all building towards an initiative for comprehensive digital literacy. Only then can we cultivate a digital environment that protects their children's privacy, dignity, and developmental needs-their very own future.