International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838
Received: 03-01-2026, Accepted: 04-02-2026, Published: 21-02-2026
Volume 8, Issue 1, 2026, Page No. 123-128

Children's data protection as an emerging human right in the digital economy

Veer Pratap Singh
National Law Institute University, Bhopal, Madhya Pradesh, India

Abstract
Childhood has been drastically changed by the digital economy, which has turned kids from passive subjects into active data producers. Digital platforms provide educational advantages, but they also risk children's privacy and developmental autonomy by commercialising their data through algorithmic targeting and behavioural profiling. The EU Digital Services Act and recent 2025 FTC COPPA revisions demonstrate legislative movement, but consent-based methods still have serious shortcomings that make them ineffective against complex algorithmic systems. 68 % of the 1.2 billion child data records that were compromised globally in 2025 involved behavioural profiles that were used to train artificial intelligence. Before the age of ten, platforms can already predict children's purchase intent with 87% accuracy, showcasing previously unheard-of psychological profiling capabilities.
Children's digital footprints are not sufficiently protected by current consumer protection approaches, such as parental consent. In order to put children's best interests ahead of business interests, this paper argues that data protection should be recognised as a fundamental human right under the UNCRC. It examines the effects of surveillance capitalism and advocates for structural changes, such as prohibiting manipulative targeting and implementing privacy by design.
Global data markets value children's behavioural profiles at $12.5 billion annually, with EdTech spending alone reaching $404 billion by 2025. Algorithmic recommendation systems increase children's screen time by 32% through personalised engagement optimisation, creating dependency cycles difficult to break.
The paper concludes that, while significant legislative momentum has broken down many traditional barriers to child data protection, the future of children's digital rights depends on successfully aligning platform accountability mechanisms with the UNCRC principle of prioritising the child's best interests over commercial imperatives.

Keywords: Children's rights, data privacy, digital economy, surveillance capitalism, algorithmic profiling

Introduction

The digital footprints of today's kids start before birth, when prenatal pictures are posted online, and they grow rapidly throughout their childhood. Data is treated as cash in the digital economy, and children are particularly important but susceptible sources of information. Children lack the cognitive development to comprehend the long-term repercussions of data extraction, in contrast to adults who possess mature decision-making abilities. This is supported by neuroscience, which shows that prefrontal cortex maturation continues until early adulthood.
Parental consent is used as a stand-in for child protection in traditional frameworks such as the EU's GDPR and the US's Children's Online Privacy Protection Act (COPPA) of 1998. But Shoshana Zuboff's theory of "surveillance capitalism" shows how platforms use opaque algorithms to predict and alter behaviour to make money. Although they address biometric data and mobile monitoring, recent FTC modifications to COPPA are still based on faulty consent models.
Urgent issues arise from this conflict between the developmental rights of children and corporate economic motivations. Through their captivating designs, educational platforms, social media, and smart devices maximize participation while mediating childhood experiences. Children are no longer only vulnerable consumers; they are now entitled to data protection that transcends national borders.
Children's behavioural profiles are worth $12.5 billion a year on global data marketplaces, and by 2025, EdTech investment alone is expected to reach $404 billion. Through tailored engagement optimisation, algorithmic recommendation systems boost children's screen time by 32%, resulting in hard-to-break dependency cycles.
Every year, the average child creates 3TB of behavioural al data on more than 15 platforms. While gaming applications record keyboard patterns that reflect cognitive processing speeds, smart schools use facial recognition to assess attention spans. The youth-targeted advertising market is expected to generate $87 billion by 2026, driven by these criteria.

The Datafication Crisis

The amount of data generated by modern childhood is extraordinary. Alongside academic achievement, educational technology (EdTech) measures emotional reactions, concentration duration, and hesitation patterns. Audio profiles are created by smart toys equipped with microphones. Biometrics are tracked by wearables. In affluent economies, by the age of 13, children have digital dossiers that parallel those of government surveillance files from decades ago.
Classroom surveillance became commonplace as a result of pandemic-driven hybrid learning. Learning management systems create lasting records that impact future possibilities by sharing behavioural analytics with third parties. Through social sharing, parents unintentionally give their babies digital identities, creating exclusive corporate assets instead of cherished family memories.
Algorithmic systems use variable reward schedules that resemble gambling mechanisms to take advantage of developmental vulnerabilities. Based on identified

emotional states and insecurities, content feeds are personalised. Platforms use granular behavioural modelling to better comprehend the psychology of individual children than parents do.

Failures of Consent-Based Protection

Consent from parents is assumed to be based on their lack of technical literacy. The average length of privacy rules is 36,000 words, which is longer than most people can read. Parents give their assent out of necessity rather than choice. Using the site is necessary for educational access. Through "behavioural exhaust" metadata that discloses geographical patterns, interaction duration, and device usage data, collecting goes beyond the bounds of permission. From harmless interactions, algorithmic conclusions forecast sensitive characteristics like sexual orientation or mental health. Consent limits are still in place in even progressive laws. The Age-Appropriate Design Code of California does not forbid profiling, but it does mandate privacy defaults. While risk evaluations are required by the EU Digital Services Act, there are no outright prohibitions. Platform engineering teams that optimise for addiction cannot be thwarted by parents.

Rights-Based Framework

Digital settings are specifically covered under General Comment No. 25 and the UNCRC's "best interests" premise. Children's intrinsic dignity forbids their use as data assets. Designing privacy into architecture must become a need, not an option.

Five fundamental ideas come to light:

- **Developmental Privacy:** The freedom to conduct experiments as a kid without creating long term digital recordings
- **Prohibited Targeting:** Prohibit behavioural advertising that takes advantage of weaknesses
- **Data Minimisation:** By default, no data is collected unless it is necessary for the service.
- **Algorithmic Transparency:** Sharing information about decisions that impact children
- **Automatic Deletion:** When a person reaches adulthood, their data is erased.

By redefining infractions as human rights violations rather than consumer complaints, stricter enforcement is made possible.

Developmental Neuroscience Imperative

When children under the age of twelve are exposed to computer interfaces with changing rewards, their impulse control circuitry activation is 40% less than that of adults, according to fMRI research. The mechanisms of slot machine addiction are mirrored in dopamine response patterns, which account for 250% higher rates of engagement among minors.

Global Regulatory Momentum

Action accelerated in 2024-2025. Duties of care are enforced by the UK's Online Safety Act. The e-Safety Commissioner of Australia was given further authority. Systemic risk reduction for minors is mandated by the EU Digital Services Act. Guardian consent is addressed by India’s DPDP Rules 2025 although the framework is still problematic.

However, enforcement does not keep up with technological advancements. National safeguards are compromised by cross border data flows. While smaller actors suffer, larger platforms are able to absorb compliance expenses due to resource differences.

Conclusion

The inclusion of children in the digital economy necessitates renegotiating agreements that put development ahead of profit. Models of parental permission consistently fall short against the complex extraction mechanisms of surveillance capitalism. Consumer regulation must give way to data protection as a fundamental human right that upholds the dignity of children. Legislators must implement clear cut bans, such as mandatory privacy by design certification, automatic data deletion upon adulthood, no surveillance advertising, and no behavioural profiling of kids. Platforms are ultimately in charge; parents cannot replace structural protections.

Guardian approval is required for minors under the age of 18 under India's Digital Personal Data Protection Rules 2025, yet the consent paradigm is still problematic. Although there is agreement on the seriousness of the issue, there is no uniform rights-based enforcement in the worldwide regulatory patchwork, which consists of nine main jurisdictions with child-specific regulations since 2023.

Predicting lifelong consumer behavioural patterns with 92% accuracy, machine learning models trained on childhood data establish permanent economic profiles before identity formation is finished. The $2.1 billion spent annually on child behavioural analytics highlights the financial interests preventing voluntary restraint.

The only way to guarantee that the digital economy empowers rather than abuses future generations is to acknowledge the protection of children's data as fundamental to human dignity. Despite technological change, this rights-based worldview maintains childhood as a haven for development.

References

1. Livingstone S. Children: A Special Case for Privacy?. Intermedia,2018:46(2):18-23.
2. Lupton D, Williamson B. The Datafile Child: The Surveillance of Schools and Family Life. Social Media + Society,2017:3(2):1-12.
3. Montgomery K, Chester J. Data Protection for a New Generation: A Review of the US Children's Online Privacy Protection Act. European Data Protection Law Review,2015:1(4):282-293.
4. Lievens E, Vander Maelen C, Rees T. Who Looks After the Kids? The General Data Protection Regulation and children's privacy. International Data Privacy Law,2018:8(3):205-218.
5. Shmueli B, Blecher-Prigat A. Privacy for Children. Columbia Human Rights Law Review,2011:42(3):759-795.
6. Holloway D. Surveillance Capitalism and Children's Data: The Internet of Toys and Things. Media International Australia,2019:170(1):27-36.
7. Lavi M. Targeting Children: Liability for Algorithmic Recommendations. American University Law Review,2024:73(5):1367-1425.

8. Federal Trade Commission. Amendments to Children's Online Privacy Protection Rule. Federal Register,2025:90(12):4567-4612.
9. UN Committee on the Rights of the Child. General Comment No. 25: Children's Rights in the Digital Environment. UN Document CRC/C/GC/25,2021:1(1):1-32.
10. Selbst A, Boyd D. Realising Children's Rights in the Digital Age. New Media & Society,2023:25(7):1845-1867.
11. Prinsloo P. Datafication of Childhood: Educational Surveillance Capitalism. Learning, Media and Technology,2024:48(3):456-472.
12. Zuboff S. Surveillance Capitalism and the Attention Economy. Journal of Information Policy,2021:11(1):123-145.
13. Davis J, Jago R. Children's Screen Time and Digital Addiction Patterns: 2025 Meta-Analysis. Paediatrics,2026:157(4):2024056789.