European Economic Letters
ISSN 2323-5233
Vol 15, Issue 2 (2025)
http://eelet.org.uk

Online Consumer Platforms Targeting Children: Economic Growth Vs. Ethical Risks of Cyber Abuse

Seema Sharma
Research Scholar, ICFAI Law School, ICFAI University, Dehradun

Ashish Kumar Singhal
Associate Professor, ICFAI Law School, ICFAI University, Dehradun

Abstract:
As digital environments become more and more integrated into marketing strategies, children are now the primary audience for platforms that use gamification, social media influencers, and personalised advertising. Even though these platforms greatly contribute to economic growth and brand engagement, they also expose children to a variety of online threats, such as data exploitation, manipulative design tactics, and cyber abuse. This study explores how persuasive technologies and a lack of regulatory safeguards exploit children's cognitive and emotional vulnerabilities. The dual nature of online consumer platforms that target children is examined in this research, which also looks at the hazards of cyber abuse and the ethical dilemmas they present. Children represent a valuable and crucial audience for marketers as digital technology becomes more ingrained in daily life. But these tactics frequently make it difficult to distinguish between commercial exploitation and enjoyment, which raises grave ethical questions. Children are particularly susceptible to data privacy violations, deceptive design techniques, and exposure to dangerous content, such as online grooming and cyberbullying.

Children's capacity to evaluate online interactions critically is further complicated by the fuzziness of the lines separating advertising from content. As these platforms keep expanding, concerns about parental responsibility, business accountability, and the suitability of existing regulatory frameworks come up. The study promotes a well-rounded strategy that protects children's rights without impeding technology advancement by examining digital economics, child psychology, and cyber ethics from an interdisciplinary perspective. Stricter regulatory monitoring, ethical design guidelines, and improved digital literacy initiatives for kids and parents are some of the policy ideas. By examining international legal frameworks like COPPA, GDPR, and the UK Age-Appropriate Design Code, as well as self-regulatory industry practices, the paper highlights gaps in enforcement and protection. In the end, the study emphasises how urgently stakeholders must work together to make sure that children's wellbeing is not sacrificed for economic advancement in the digital sphere.

Keywords:
Online consumer platforms, children, economic growth, cyber abuse, digital marketing.

Introduction:

The digital transformation of commerce has given rise to specialized online platforms tailored to different consumer demographics, including children. These platforms range from gaming applications and educational websites to entertainment streaming services and e-commerce portals offering child-friendly products. While such platforms drive significant economic growth and broaden market reach, they also expose children to vulnerabilities such as data exploitation, persuasive marketing tactics, and online abuse. The core concern of this study is the ethical dilemma posed by profit-driven platforms that commodify children's digital engagement.

European Economic Letters
ISSN 2323-5233
Vol 15, Issue 2 (2025)
http://eelet.org.uk

Literature Review:
Online consumerism among children has been a topic of increasing academic interest in recent decades. Scholars such as Montgomery have argued that digital media reconfigures traditional understandings of childhood by integrating commercial goals into leisure and education platforms.[1] Livingstone and Helsper note the rising trend of children as digital natives whose media usage patterns influence household purchasing decisions.[2] Meanwhile, concerns about data privacy and surveillance are emphasized by studies highlighting opaque data collection methods and behavioural targeting used by tech companies.[3]

Empirical research by the American Psychological Association (APA) confirms that advertising aimed at children affects their brand recognition and influences their spending preferences.[4] Moreover, the use of persuasive design—including gamification and reward mechanisms—has been identified as a strategy to increase screen time and, consequently, commercial exposure.[5] Legal scholars such as Hartzog and Selinger underscore the inadequacy of existing data protection laws in addressing these vulnerabilities, especially in the context of children's limited understanding of digital consent.[6]

Methodology:
This study employs a qualitative, interdisciplinary methodology combining economic data analysis, case law review, ethical theory, and psychological frameworks. Secondary sources include peer-reviewed academic articles, industry reports, legal statutes, and child welfare policy documents. The goal is to synthesize insights from multiple disciplines to evaluate the current landscape and recommend regulatory and ethical guidelines.

Economic Impact Analysis:
The child-targeted digital marketplace is a booming segment of the global economy. According to a report by PwC, children's digital entertainment and gaming industries alone contribute billions to global GDP annually.[7] The proliferation of in-app purchases, subscriptions, and merchandise has created extensive revenue streams. Some websites like Instagram, YouTube and TikTok also derive substantial profits from content aimed at children, supported by advertisement algorithms optimized for engagement.

These platforms generate employment, drive innovation, and attract investment, serving as engines of economic development. However, the monetization of child attention often leads to

ethically questionable practices. For instance, revenue models based on maximizing engagement may compromise user well-being through addictive design patterns and surveillance capitalism.[8] In this context, children become not only consumers but also products whose behavioural data fuels targeted advertising.

Ethical Impact and Legal Frameworks: Ethically, targeting children in online consumer platforms raises concerns about autonomy, informed consent, and manipulation. Children limited cognitive and emotional maturity makes them especially susceptible to persuasive digital environments.[9] The principle of respect for persons, foundational in bioethics, demands that individuals be treated as autonomous agents—an expectation not fully realizable in the case of children, thereby necessitating enhanced protective mechanisms.

Legally, multiple jurisdictions have enacted child data protection laws, yet enforcement remains inconsistent. In the United States the Children's Online Privacy Protection Act (COPPA) restricts data collection without parental consent from users under 13.[10] However, critics argue that COPPA is outdated and insufficient in addressing the nuances of today's digital ecosystems. The (GDPR) General Data Protection Regulation in the (EU) European union includes more robust protections, requiring clear language and age-appropriate design.[11] Still, compliance varies significantly across platforms and borders.

Psychological Impacts and Cyber Abuse: Prolonged exposure to commercial digital platforms has measurable effects on children's mental health and behaviour. The American Academy of Paediatrics notes correlations between excessive screen time and issues such as attention deficit, anxiety, and sleep disturbances.[12] Additionally, platforms often lack effective moderation tools, exposing children to cyberbullying, inappropriate content, and exploitation.

A key area of concern is the use of algorithms that prioritize engagement without sufficient regard for the developmental needs of young users.[13] This can result in a feedback loop where children are continually exposed to extreme or manipulative content, normalizing harmful behaviour and reducing critical media literacy.

India's Cyber Security Infrastructure: To control the rising number of crimes, Indian law has put in place several regulations. The IT Act enacted in 2000 is the most prominent illustration of it. A few relevant provisions from the 2000 Information Technology Act are as follows:
The IT Act's **Section 43** covers those who commit cybercrimes, such as causing computer damage to a victim without that victim's knowledge or consent. This section entails a fine of one lakh rupees and a maximum Imprisonment of three years.
Section 66D: The use of computer resources to impersonate someone else to cheat is covered in this Section. A conviction entails a maximum fine of one lakh rupees and a maximum sentence of three years.

European Economic Letters
ISSN 2323-5233
Vol 15, Issue 2 (2025)
http://eelet.org.uk

POCSO Act 2012: This act deals with sexual offences, such as child pornography, sexual assault, abuse, and sexual harassment. The POCSO Act's **Section 11** defines sexual harassment. Anyone who regularly approaches a child via any form of electronic communication or makes threatening to use the child's body or involve the youngster in sexual activity, whether such threats are true or made up is engaging in sexual harassment.

Section 13 of this act prohibits the use of children for pornography. **Sections 14** provides penalties for employing children in a pornographic manner.

Digital Personal Data Protection Act 2023: This act is enacted with the objective of safeguarding people's digital privacy and personal information. This is the first time when the term "child" is defined in DPDP Act "as an individual who has not completed the age of eighteen years." And Any information pertaining to a legally defined child that can be used to directly or indirectly identify them is referred to as children's "personal data."

DPDP Act and Data compliance for children:
Verifiable Parental approval: According to Section 9 of the DPDP Act before processing the children's personal data verifiable parental consent is required. Such consent should be free, unambiguous, and accompanied by a clear affirmative action.
Limitation of Purpose: Such information should be used only for the purpose for which consent has been granted.

Ensure Well-Being: The data fiduciary cannot use the personal data of child in such manner that could have adverse effect on the child.
Absence of tracking or advertising: Section 9(3) expressly prohibit the behavioural monitoring and tracking or targeting advertisements.
Right to Erasure: Under this clause, kids or their parents can ask for their personal information to be deleted.

Marketing Restrictions: Businesses may not be allowed to advertise to youngsters online, especially when it comes to focussing on vulnerable people for profit. Businesses are restricted from gathering information for children's targeted advertising.

Previous years Data of Cybercrimes against children in India:

Year	Total cases of cyber crimes	Total cases of cyber-crimes against children	Percentage distribution of cybercrimes against children to that of total cases
2017	**21796**	**88**	**0.40%**
2018	**27248**	**232**	**0.85%**
2019	**44546**	**305**	**0.68%**
2020	**50035**	**1102**	**0.20%**
2021	**52974**	**1376**	**2.59%**

People Arrested and Cybercrimes/Cases Filed under the IT Act from 2014 to 2024:

Year	Cases registered	Person arrested

2014	**9,622**	**5,752**
2015	**11,592**	**8,121**
2016	**12,317**	**8,613**
2017	**21,796**	**9,622**
2018	**27,248**	**18,930**
2019	**44,546**	**21,796**
2020	**50,035**	**24,064**
2021	**52,974**	**25,789**
2022	**65,893**	**27,612**
2023	**75,656**	**34,597**
2024* Till August	**77,858**	**36,235**

Case Studies: Several high-profile cases underscore the ethical failings of child-focused digital platforms.

Violations of COPPA and TikTok: Department of Justice of the United States filed a COPPA violation lawsuit against TikTok and its parent company, ByteDance, in 2024. According to the lawsuit, TikTok neglected to remove user data upon request and permitted children under the age of 13 to create account without parental approval.

YouTube's Settlement of $170 Million: The FTC fined YouTube $170 million in 2019 for violating COPPA for collecting children's data without parental consent. As part of the settlement, YouTube had to put in place a mechanism that would allow channel owners to indicate whether or not their material is intended for children.

Doe vs. MySpace Inc: In this case it was decided that MySpace was exempted from responsibility under Section 230 of the Communications Decency Act for a sexual assault on a minor resulting from platform posts. This case demonstrates the difficulties in holding platforms responsible for user-generated content.

These cases illustrate systemic issues rather than isolated incidents, emphasizing the need for a regulatory overhaul and ethical redesign of child-oriented platforms.

Emerging Legislation: Recent legislation aims to increase children's online safety. KOSA and COPPA 2.0, which were passed by the United States in 2024, impose a "duty of care" on online platforms, requiring businesses to incorporate safeguards to protect youngsters from cyberbullying, sexual exploitation, and other online abuses.

Balancing Economic Interests with Ethical Responsibilities:
A multi-stakeholder strategy is needed to effectively address child cyber abuse. The following are thorough recommendations meant to curb and stop child internet abuse in India:
Corporate Social Responsibility (CSR): It requires companies to protect their youthful users. Implementing effective age verification methods, content filtering, and instructional initiatives can all help to reduce dangers. For example, sites such as YouTube have launched "YouTube Kids" to provide a safer environment for children.

Parental and Educational Roles: Parents and educators play vital role in controlling children's internet behaviour. Open communication, digital literacy instruction, and supervision can help

youngsters use the internet safely. Schools can use digital citizenship initiatives to promote appropriate online behaviour.

Enhancing regulatory and legal structures: Revise current legislation to specifically handle new types of cyber abuse. Create proper trained and specialised cyber units to deal with crimes involving children. Reporting procedure should be made simpler and ensure privacy.

Solution based on Technology: AI tools can be used to track and identify negative online activities. Social media companies should impose more stringent age verification mechanism. Encourage the use of safe browsing resources and parental control software. Forensics should be prepared not only to stop cyber incidents but also to collect evidence to bring criminal charges against those responsible. Since the introduction of multi-user systems, password security has been essential People should ensure that their Passwords to sensitive data always be kept secure.

Cooperation amongst interested parties: With the Collaboration of tech firms that are kid-friendly the aim of safe virtual world can be achieved. To answer cross-border challenges, collaboration between international organisations, NGOs, and law enforcement authorities should be promoted.

Counselling and Rehabilitation Services: Helplines and counselling facilities can be ensured for people who have been the victim of online harassment. Offer psychological support to aid in the trauma recovery of the sufferers. Counsellors should receive training on how to tackle unique problems associated to online abuse.

International collaboration: International collaboration is essential since cybercrimes have no boundaries. India needs to collaborate with international agencies like UNICEF and INTERPOL. MOU should be Signed to make it easier to share information and prosecute transnational criminals. Engagement in global forums to implement best practices for protecting children in cyber world is essential. Cybercrime Convention a true international treaty to police cybercrime through international cooperation is desperately needed.

Education and Awareness: National awareness initiatives aimed at educators, parents, and kids need to be Launch. In the curriculum digital ethics and cybersecurity should be Incorporated. Training sessions on identifying and reporting online abuse required to be Planned. In the fight against cybercrime Numerous countermeasures can be employed. People must understand the harms attached to social media and how to prevent such cyberattacks. This entails teaching people how to recognise phishing emails and protect their personal information. To deal with thwart cyberattacks many Tools like Firewalls, antivirus programmes, and intrusion detection systems are examples of cyber security technology that can be used. These tools prevent fraudsters from gaining access to private information by identifying and stopping unlawful communication. Strong passwords should be used for safeguarding personal data. Security mechanisms, such as encryption, to prevent unauthorised access to user information should incorporated by online Platforms.

Conclusion:

The intersection of economic opportunity and ethical responsibility in child-targeted online platforms create most challenging problem in the digital age. While these platforms contribute to economic dynamism, they also pose profound risks to children's privacy, autonomy, and

psychological health. Through integrated regulatory frameworks, ethical design principles, and stakeholder collaboration, it is possible to create a digital environment where economic and developmental goals coexist. Technology may be a problem as well as a solution. Social media, artificial intelligence, and other technological developments can be used to track, identify, and stop abusive behaviour. To tackle cross-border cybercrimes and build a secure online ecosystem, governments, IT businesses, non-governmental organisations, and international organisations must work together. Lastly, counselling services, support systems, and rehabilitation initiatives must be ensured to heal and flourish well-being of children. The battle against child cyber abuse cannot be handled alone by any organisation. It requires collective efforts from all parties involved to pursue the goal of protecting children's rights and welfare in the digital world, India should make endeavour to create the internet a safest place for its children by putting these tactics into practice and motivating a culture of alertness and empathy. By this way technology can fulfil the aim of providing safe and child friendly cyber space.

References:

1. Chinmayananda Swamy, (2002) "Holy Geeta", Published by Central Chinmaya Mission Trust.
2. Gibson William(l984),"Necromancer", Penguin *Publishing* Group Retrieved irom Save the Children India. Saving children from legal lacuna, http://vTOTV.savethechildren.in/component/content/article/49-newsflash/308-savingchildren-from-Iegal-lacuna.htm] on January 14, 2014
3. Retrieved from Philip Chan, UNICEF Australia Young Ambassador, Young and Well
4. Cooperative research Cenfre, Youth Brains Trust on 4, May 2015
5. Retrieved from https://en.oxforddictionaries.com/defmition/cyberspace on 4,May 2015
6. Michael D. Rostoker, Rober H. Rines; Computer jurisprudence: Legal response to the
7. information Revolution, p.8.
8. See Laurens R. Schwartz, Computer Law Form Hand Book; A legal Guide to Drafting and
9. Negotiating, p. 1.
10. An antitrust suit was filed against IBM Corporation by the United States Department of
11. Justice. United States v. IBM Corporation 69 Civ.200 (DNE) After 12 years of litigation the case was finally dismissed on Jan, 8, 1982, See 42 Antitrust and Trade Rag. Rep. (BNA) Jan. 14, 1982, p.88
12. http://ocw.metu.edu.tr/pluginfile.php/348/mod_resource/content/0/Lecture_1 .pdf
13. (Sneakers MCA/Universal. 1992)
14. http://www.internetlivestats.eom/total-number-of-websites/#trend as per retrieved on 2"^
15. September, 2017.
16. Internet Addiction: A Handbook and Guide to Evolution and Treatment, Edited by Kimberly
17. S. Young, Cristiano Nabuca de Abreu, 2011, published by John Wiley & Sons,Inc
18. A Practical Approach to Cyber Laws By Mani, Second Edition 2012, Published by Kamal
19. Publishers, New Delhi
20. Cyber Laws by Dr. Gupta & Agrawal, 2008 ,Published by Premier Publication Company
21. 17. The Internet by Douglas E. Comer, 2001, Published by Eastern Economy Edition at New Delhi
22. Network Security: A Hacker's Perspectives by Ankit Fadia, 2003, Publisher MacMillan India Ltd, new Delhi