International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Children's Rights Perspective on Privacy and Data Protection in the Digital Age

Vedanshi Verma[1], Anugya Mishra[2]

[1,2]GGSIPU

Abstract

The rapid evolution of digital technologies has significantly impacted children's lives, transforming how they engage with information, interact with others, and build their identities. This paper explores the intersection of children's rights, privacy, and data protection in the digital age, focusing on the emerging challenges and risks they face. From the rise of "sharenting" to the exploitation of children's personal data, the paper highlights the tension between parents' rights to free expression and children's right to privacy. Additionally, it examines the role of global legal frameworks such as the United Nations Convention on the Rights of the Child (UNCRC) and the General Data Protection Regulation (GDPR) in protecting children's digital rights. The analysis provides insights into how current regulations are addressing these challenges and proposes legal reforms and best practices to safeguard children's privacy in an increasingly interconnected world. By centering children's best interests, this research calls for a balanced approach that respects both the responsibilities of parents and the autonomy and dignity of children in digital environments.

Introduction

In today's globalized world, children often make their Internet debut before they are even born, usually appearing on their parents' social media platforms as hazy ultrasound images. Though these children may become aware of their digital footprint and online identity at an early age, they remain powerless in asserting their rights, with parents assuming the "dual role of parent and publisher". This responsibility births an inherent conflict between a child's right to privacy and a parent's right to freedom of publication — putting children and their development at risk.

This article will provide a brief legal and practical analysis of this conflict. It begins by outlining the basis of children's rights to privacy and parental rights to freedom of publication, before analysing the nuances of the conflict. The article concludes with some proposed legal solutions to the existing standoff and offers a list of best practices for parents engaged in sharenting (the word stems from parenting and sharenting) to consider. It is hoped that this work will contribute to a growing dialogue on the risks of sharenting and the importance of centring the best Interests of children in all sharenting discussions.

Literature review

According to the United Nations Convention on the Rights of a Child (UNCRC), a child is any human below the age of 18 (Article 3, Part 18) and the vital role that digital technology plays in the lives of modern children cannot be over-emphasized. Children's usage and access to information has changed with the integration of computer technology; although multiple researchers have worked on improving access and discovering patterns of usage, the vast majority of the works have focused on adult.

Objectives

To Understand Children's Rights in the Digital Age
To Identify Challenges and Risks Faced by Children in the Digital World
To Examine Legal Measures to Protect Children's Rights
To Assess International Cooperation and Challenges

What is Sharenting?

Sharenting is often described as any instance where an adult – in charge of a child's well-being – "transmits private details about a child via digital channels" Though the term is conventionally used to refer to social media and common telecommunications channels, children's information can also be input into other data tracking tools such as fertility applications, smart toys or personal cloud servers.

Due to the widespread accessibility of technology and Internet access, the average child has a digital footprint before their first birthday, typically in the form of an ultrasound image or birth announcement photo. This information is not limited to images; date of birth, name, geographic location and school are important to data brokers who often sell personal data to advertisers.

Sharing is a feature of modern parenting that represents the transition of family traditions (like children's books and family photo albums) into the digital sphere. The danger of this changing way of writing and sharing child development is that the audience is now wider than ever and the message can spread (whether intentionally or unintentionally) and sometimes get into the hands of children. In addition, children are forever marked with these "digital tattoos" that they do not approve of, and this can negatively affect their development.

Sharing can be useful in some situations. For example, parents of children with disabilities can share their experiences with each other and compare reports on how they can support their children. Still, there is a big risk. Parents are losing control over bullying and criticizing their children for what they say online; YouTube frequently removes videos featuring children due to fear of violence; Public information about children's behavior and whereabouts makes them vulnerable to paedophilia, child abduction and other crimes targeting this group.

Online data risk becomes even riskier because posted photos and videos can remain online indefinitely without the child's consent. Finally, it is difficult to analyse the impact of sharing because the impact of sharing may not be immediate, even though it poses a danger to children or is a constant of information that can be used later.

Children's right to privacy

Article 16 of the United Nations Convention on the Rights of the Child (UNCRC) states: "No child shall be arbitrarily or unlawfully deprived of his or her personal life, of his or her family, of his or her home, or of the right to write. a child shall not be unlawfully or unlawfully affected by himself, his family, his home or his writing. "His dignity and reputation" and "The children have the right to be protected against interference and attack." (UNCRC, 1989)[1] For example, the right to be forgotten in Article 17 of the Convention The EU General Data Protection Regulation (GDPR, 2016)[2] explains the importance of privacy and data protection for children's development.

[1] Convention on the Rights of the Child, 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990)
[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)

The European General Data Protection Regulation provides effective standards. Internet users, including children, should be given clear and transparent instructions explaining to children how their data will be collected and processed, he said. He said everyone, including children and young people, should be able to access their personal information and have the opportunity to correct inaccurate information.
Sharing that normalizes the observation of children is a serious violation of privacy and personal privacy and causes children to be unable to determine their own images.

Parents' right to freedom of expression

While children's privacy rights are violated in the same way, parents' right to freedom of expression as granted by Article 13 of the UNCRC (UNCRC, 1989) is also violated. Parents are the first defenders of their children – children who are too young and do not have the necessary maturity, experience and ability to make decisions or make decisions in life. Therefore, parents should act as the best guardians for their children, especially those who are "most interested in memory."
It is also important that children are seen as independent individuals who are independent and not dependent on their parents. If the parent-child relationship is not viewed in this way, the child's interests will be affected and the selfishness of the parents will be prevented. This may mean that the parenting options involved ignore your best interests. The Convention on the Rights of the Child recognizes the importance of privacy, freedom and harmony within the family, but in this context children's rights mostly depend on their parents and do not provide them with special protection.
Normally, parents will and should play a responsible and careful role in influencing their children to enter the online world. Many parents have restricted their children's online use and require schools and organizations to obtain permission before sharing photos or information about their children online. But children often don't have the opportunity to "unplug" when they want to separate themselves from the digital world. Not being able to distinguish between the public world and the private world is dangerous and opens the door to all kinds of physical or online abuse. Children (e.g. digital kidnapping – the online theft of a child's personal identity by someone believed to be their child).
When information about a child is shared without permission, parents become the narrators of their child's story, leaving the child vulnerable and unprotected. Children's privacy is also the dignity and respect of children. There may be a backlash from the current generation of young people who will try to attack them and criticize their parents for creating negative images online without permission. It's safe to say that some parents often sacrifice their children's privacy to enhance their online identity.

Violations of children's rights and the development of harmful information: Who is responsible?

The concept of digital citizenship is an argument that technology companies often use to commit themselves to the responsibility of protecting children from crime by accessing information through home or classroom learning and in public discussions with them. Individual terms of use and privacy are almost invisible. However, in case of misuse of children's personal information in the digital environment and violation of their rights, the greatest responsibility should not fall on the parents, because they are either good at social media or do not know it at all. The most important thing to consider in this case is the inequality between companies and families, as well as the fact that most people do not understand the complexity and quality of digital relationships and business models in this field. Therefore, it is important to understand the different types of harmful digital uses of children's personal data by businesses and demonstrate their impact on children's growth.

Child Abuse Cases Confidential Information

The tragic case of Meghan Meyer[3] in the United States demonstrates the serious consequences of bullying in cyberbullying. Megan, 13, committed suicide after being bullied by a fake online profile created by an elderly relative. Information about the urgency of combating cyberbullying and protecting children from online bullying.

Recently, the Madras High Court in S. Muthukumar Petitioner(S) v. TRAI case[4] ordered the central government to ban the above-mentioned apps for allegedly displaying pornography and pornography. Music and video creator app Tiktok has been fined by the US Federal Trade Commission (FTC) for allegedly collecting personal information from children under the age of 13 without parental consent. Likewise, the lack of online laws to protect children's online rights puts a security blanket on the app and Tik Tok is saved. A similar incident occurred when Tik Tok was again questioned by the judicial body, the National Commission for Women, for the publication of acid attack videos. Such cases reveal how children's online privacy rights are compromised by online practices due to the lack of appropriate laws.

The Supreme Court in the case of Re Exploitation of children in orphanages in State of Tamil Nadu v/s Union of India[5], held that the use of technology will help solve important problems such as finding missing children, rescuing people working in dangerous trades and victims of child abuse.

"As we all know, our country is a technological powerhouse, and if we cannot leverage the resources and use technology to benefit children through computers and the Internet, then our status as a technological powerhouse will be compromised, and only in form," the judge said.

Another situation is when children create their own social media accounts and share/re-share images of themselves, their families, friends, contact information, thoughts, interests, of which they are not aware and are not ready to deal with the consequences. They are often susceptible to trolling that produces invisible and strange results that most children cannot do. This problem is exacerbated by the fact that it is almost impossible to delete information in digital media. This concern S.K. It is very well expressed by. As Kaul, J. observed: (K.S. Puttaswamy Case[6], SCC Page 17) 630, para 631)

• Recently in Aadhar judgment, the Supreme Court recognised the "Right to Privacy" as an intrinsic part of the right to life and personal liberty provided under Article 21 of the Constitution of India

Legal and Safety Risks Posed by Parental Oversharing

It is estimated that by 2030, more than 66% of identity fraud cases will have resulted from sharenting (Hsu, 2019). This idea is supported by AVG Antivirus who anticipate a growth in identity theft the more parents share their children online (Meakin, 2013). Uploading and sharing child information exposes children to the risk of photos going viral and falling into dangerous hands and fraudulent activity among other dangerous outcomes (Hopegood, 2020). In fact, Barclays Bank predicts that by 2030 $867 million will be lost to fraudulent information garnered from sharenting.

Broadly, there are four categories of harm that sharenting may lead to:

1. Tangible harms – these include digital kidnapping, identity theft, fraud and data collection (Steinberg, 2019);
2. Children's rights violations – this includes infringements on the right to a private family life (Steinberg,

[3] **United States v. Drew**, 259 F.R.D. 449 (C.D. Cal. 2009)
[4] 2019 SCC ONLINE MAD 24317
[5] 2013 AIOL 833
[6] AIR 2017 SC 4161

2019);
3. Digital citizenship harms – these relate to the importance of child privacy and data protection (Steinberg, 2019);
4. Intangible harms – these relate to the mental harms inflicted upon children which negatively affect their development.

Best Practices for Parents

Children's early existence as online entities affect their ability to develop a self-awareness and sense of identity. If parents want to adequately protect their children from the dangers of sharenting they must, at the very least, recognise their inherent risk in the first place. At best, parents can stop sharing. However, if they engage in this behaviour they should be mindful of the privacy of all shared content (who owns it and who has access – this can be viewed using a third party website such as mypermissions.org) and ensure they use search. Aggregators find information about their children that they can organize.

Parents should cultivate social media users and read relevant privacy policies to ensure they use their maturity to make informed decisions on behalf of their children. Before sharing information, parents should exercise caution and avoid: Sharing sensitive images of children (such as near-nude photos) that could be dangerous; close physical space that could cause physical harm to children; and details to be anonymous.

Sharing is a new phenomenon; Until policymakers find ways to regulate these activities, parents must protect their children at all costs. Children should be treated with respect and privacy, their interests should be protected at all times, recognizing their independence.

Privacy Bill 2019: Provisions for protecting children's online information

After a long time, the government introduced the first Privacy Bill 2019 to Parliament in December 2019. This Privacy Policy aims to protect personal data and establish a data protection system for children. This is the purpose. Article 4 of the Privacy Law provides for the processing of children's personal data and sensitive personal data. It also provides that the processing of personal data will be carried out by the government, Indian entities and foreign companies processing personal data (collectively, "data fiduciaries"). Article 16 of the Law determines the framework of the study. It recommends that all parents should act in the child's best interests and protect the child's rights. The information surrogate must verify the age of the child and, if the child is a minor, obtain parental consent before processing any personal information. This policy refers to data controllers who use online commercial services or children's websites as "controllers" to learn or process big data. Caregivers who provide counselling or child protection do not need to obtain parental permission. These regulations are supposed to turn schools and counselling centres into "guardian" positions. The Data Protection Authority is a supervisory authority established in accordance with the provisions of the Law, with the authority to protect personal interests and prevent the misuse of data. If the trustee is found to have processed documents unlawfully or illegally, a fine of Rs 15 billion or 4% of the total annual income, whichever is higher, will be imposed.

Since the law has been passed and become a legal bill due to the impact of the epidemic, children's privacy rights must be protected with the provisions of the bill.

Conclusion

The digital environment, although complex and dynamic, is an important place for children's socialization.

Their protection and safety in cyberspace cannot be the responsibility of parents and guardians alone and cannot be ensured by informed media and responsible, knowledgeable users. Service and product production is crucial. It creates a framework within which children can express or fail to express their abilities, identities, and rights. It's the means through which children will find a safe and caring environment or experience the permanence of an enterprise version with severe violations of their rights through practices that allow privacy and safety violations, financial exploitation, freedom violations, and discrimination.

Consequently, tech companies have an obligation under the CRC (Convention on the Rights of the Child) to recognize, defend, promote, and fulfill the rights of children and their best interests in all decisions related to data governance of their services or products. The adoption of a **Children's Rights by Design (CRbD)** standard for data use is more than a vital self-regulatory practice; it is engrained within the CRC's international legal provisions, even making it feasible for companies to participate in mechanisms for monitoring the implementation of the CRC by the UN Committee on the Rights of the Child. The effective implementation of a **Children's Rights by Design** standard for data use by tech companies is an imperative step towards fair, just, and reasonable governance of children's data and the overall protection and promotion of their rights.

Key Findings and Insights:

The massive exposure and smooth transit of youngsters' non-public information and continual identifiers – such as name, cope with, smartphone quantity, e-mail deal with, biometrics, photographs, films, audio recordings of the kid, IP addresses – that can be used to music a infant's places and sports over time and throughout unique websites and on line services, pose several threats to their physical, intellectual and sexual integrity, particularly via non-authorized and malicious touch, amplifying the threat of offline abuse.

As an instance, easy get admission to to infant sexual abuse materials and insufficient identification of and action to combat grooming and predatory behaviour in on line spaces enables the exponential increase of dangerous practices, such as online sexual exploitation and abuse.

The shortage of online safety through layout and the misuse of kids' non-public records for harmful and predatory behaviour in digital structures and services, search engines like google, livestreaming technologies, social media, chats, message apps and interactive video games increasingly more have an effect on youngsters' fitness and improvement and may have lifestyles-long impacts that still contain their families and all society.

Therefore, it needs to be mentioned that the measures presented underneath must continually be continuously tailored to make certain safety because of fast and occasionally disruptive technological development.