Protecting Children's Privacy in the Digital Age: Indian Regulations and Challenges

---

Abstract

The paper seeks to understand the contextual vulnerability of children in the digital ecosystem. This is done through understanding current issues through a conceptual understanding of privacy. Children constitute the most vulnerable stakeholders due to their lack of knowledge about privacy laws coupled with lack of legal attention being given to their interests. The paper seeks to highlight the shortcomings in existing data protection laws in India with respect to digital rights of children. We compare the Digital Data Protection Act in India to its European counterparts. Policy recommendations are arrived at through examination of provisions of other countries and adapting them in the Indian legal framework.

The policy recommendations explored include both structural and legal changes. The structural changes consist of setting up a nodal agency for data protection. It is required to publish regular reports regarding data breaches to ensure accountability of data controllers. Similarly, the mechanisms for age verification need to be improved in order to reduce under-age subscriptions to social media sites. The law must also define detrimental interests of children to prevent the invasion of children's rights by the data controller. There should also be Data Protection Impact Assessment in order to identify the vulnerabilities

Introduction

In January 2023, there was a data breach on the website of Digital Infrastructure for Knowledge sharing app (DIKSHA). This is an app launched in 2017 to facilitate learning through online modules and interactive material. The cause of the data breach was that the cloud server storing data was left unprotected. Data compromised included personal information of both students and teachers. The full names of students and the area of school in which they studied was revealed. This is just one instance of children's data being available in the public domain due to lack of adequate security of data servers [1].

Vulnerability of children in the online space is a global phenomenon. A report by Human Rights Watch (HRW, 2022) observes that 89% of EdTech products around the world engage in predatory data practices, putting children's data at risk[2]. Most EdTech companies send children's personal information to third party advertising

[1] Elliott, V. (2023). *A Major App Flaw Exposed the Data of Millions of Indian Students*. Wired. https://www.wired.com/story/diksha-india-education-app-data-exposure/

[2] *Online learning products enabled Surveillance of children* . (2024). Hrw.org. https://www.hrw.org/news/2022/07/12/online-learning-products-enabled-surveillance-children#:~:text=Human%20Rights%20Watch%20released%20technical

companies. This empowered the third party company to track an individual's searching pattern and give out targeted advertisements. In this hostile online environment where the demand for children's information is high, it is necessary for the government to come up with measures to specifically protect the data of children. However, the same study conducted by HRW revealed that 39 out of 42 governments procured the services of such EdTech companies. Some governments took a step further to make the use of such softwares mandatory [3]. It is in this context that we need to study the position of children in India's data protection framework. We look at the vulnerabilities which children face in the digital framework and why there is a need to pay special attention to their data. We subsequently lay down the legal evolution of the concept of privacy. We conclude by providing a comparison with the legal framework of other developed countries and provide policy recommendations on the same.

Evolution of theory of privacy

Privacy is a central subject for discussions surrounding information security, datafication of individuals and privacy threats posed by Big data. The diverse connotations and lack of theoretical literature adds to the ambiguity of the concept. The operationalisation of privacy as a theoretical construct occurred through legal rather than philosophical interventions[4]. The absence of privacy as an explicitly core concept in the classical liberal tradition implies that it carries an instrumental rather than intrinsic value. It is instrumental for the realization of another core value i.e security. Not being a core concept, its conceptualisations cannot be universal and culture agnostic. The situational worth of privacy varies across cultures leading to creation of different zones of privacy. In other words, it is a fluid concept [5].

The idea of privacy being an exclusive concept has been questioned by Thomson (1975), who argues that privacy is a cluster of rights which is marked by an overlapping of existing rights. It is a derivative right in the sense that it can only be described in relation with other rights[6]. Such interest based

---

[3] Hye Jung Han. (2022, May 25). *"How Dare They Peep into My Private Life?"* Human Rights Watch. https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments#_ftn82

[4] McCloskey, H. J. (1980). Privacy and the Right to Privacy. Philosophy, 55(211), 17–38. https://doi.org/10.1017/s0031819100063725

[5] Moor, J. H. (1997). Towards a theory of privacy in the information age. ACM SIGCAS Computers and Society, 27(3), 27–32. https://doi.org/10.1145/270858.270866

[6] Thomson, J. J. (1975). The Right to Privacy. Philosophy & Public Affairs, 4(4), 295–314. https://www.jstor.org/stable/2265075

conceptions of privacy argue that there is a lack of philosophical or legal grounding necessary to justify them as rights [7]. The characterisation of privacy as rights has evolved in its meaning and implications. It can be broadly classified into: non intrusion, seclusion, control and limitation. The former two conceptualisations misconstrue privacy with liberty and secrecy respectively. The connotation of privacy based on control provides more nuance to the definition of privacy. It provides moral agency to the data subject to have control over their Nonpublic Personal Information (NPI)[8]. Nissenbaum provides a critique of the protection of private information, calling for definition of privacy as contextual integrity. All data available in the public domain need not be seen as public data, the dividing line between public and private data varies across social contexts [9]. The blurring lines between public and private sphere is exemplified by the communication privacy theory which is represented by the public by-default nature of personal communication.

Vulnerability of Children in the current digital environment

Internet being a largely inequitable space, its ramifications differ across age groups and social groups. On the 25th anniversary of the World Wide Web (WWW), the founder called for a bill of rights to guarantee some degree of net neutrality and freedom. There is a direct correlation between opportunities and consequent risks associated with the internet. It is designed in such a way that makes children more vulnerable to online threats [10]. There are a multitude of factors which affect the privacy of children. Online risks specific to children can be classified into the following categories: mediation by parents, advertisement related risk and internet technology risks. The classification of risks into categories is important because the nature and magnitude of risk is different for each category. Mediation by parents puts the notion of consent of children under threat whereas advertisements can

[7] The Handbook of Information and Computer Ethics. (2008). https://doi.org/10.1002/9780470281819

[8] TAVANI, H. T. (2007). PHILOSOPHICAL THEORIES OF PRIVACY: IMPLICATIONS FOR AN ADEQUATE ONLINE PRIVACY POLICY. Metaphilosophy, 38(1), 1–22. https://doi.org/10.1111/j.1467-9973.2006.00474.x

[9] Nissenbaum, H. (1997). Toward an Approach to Privacy in Public: Challenges of Information Technology. Ethics & Behavior, 7(3), 207–219. https://doi.org/10.1207/s15327019eb0703_3

[10] Livingstone, S., & Bulger, M. (2014). A Global Research Agenda for Children's Rights in the Digital Age. Journal of Children and Media, 8(4), 317–335. https://doi.org/10.1080/17482798.2014.961496

extract personal data from children.

Mediation by Parents

The Convention on Right of Child (CRC), which is a legal-international recognition of children as active stakeholders in protection of their own rights. In practice, parents play a role in mediating their child's digital engagement. Mediation of digital interactions occurs in a spectrum: it ranges from a total control over the content being consumed to a limited choice being provided to the children in terms of freedom to use the internet [11]. The dependence of children on their parents is often seen as natural and unavoidable. The impact of mediation is that parents, who are themselves not well aware of privacy rights are consent bearers for their children. This often takes the form of posting pictures of their infants and posting them on social media. This will leave a child's nonconsensual digital footprint on the internet till they attain maturity. Children are often surveilled by their parents to ward off any potential privacy threat [12]. There is a tendency of children to prioritize privacy from parents as compared to strangers on the web[13]. This is known as the **privacy paradox** in which the primary interest of the child is privacy from the parents while the primary concern for parents is privacy from online predators.

Advertisements

Children below the age of 7 years lack the intellectual acumen to recognise the persuasiveness of advertisement, which they only develop between the age of 7 and 11. This does not imply that they are able to resist such commercial efforts. Advertisers exploit such an impressionability in order to sell their product. They use emotional appeals to establish relatability with their users. Micro-advertising can manifest through advergaming or online privacy invasive practices such as data profiling.

---

[11] Dias, P., Brito, R., Ribbens, W., Daniela, L., Rubene, Z., Dreier, M., Gemo, M., Di Gioia, R., & Chaudron, S. (2016). The role of parents in the engagement of young children with digital technologies: Exploring tensions between rights of access and protection, from "Gatekeepers" to "Scaffolders." *Global Studies of Childhood*, *6*(4), 414–427. https://doi.org/10.1177/2043610616676024

[12] The Protection of Children Online. (2011). OECD Digital Economy Papers. https://doi.org/10.1787/5kgcjf71pl28-en

[13] Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). Children's Data and Privacy Online Growing up in a Digital Age an Evidence Review. https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf

Advergaming is a phenomenon in which online games are used as a means of advertising a product or service. Advergaming operates in a manner which cannot be easily recognised by children as a form of advertising. Children often fall prey to inappropriate games and products which are presented to them through mechanisms of advergaming. An analysis of the apps meant for children below the age of 5 on Google Play revealed that 96% of them contained some sort of hidden advertisements and incentives which improve game performance (free tokens or advanced features) [14].

Ostensibly, the Social Network Sites are without subscription fees. Instead, their financial model is based on advertisement derived revenue which is referred to as datafication. **Datafication** involves collection, profiling and processing of subject information not restricted to browsing patterns. It encompasses the time stamps and GPS location. Third party information collection can be through clickbaits (for eg. quizzes) and likes. A study by Europa Commission (2010)[15] revealed that embedded advertisements have a subliminal impact on children without them being consciously aware of it. It also revealed that children have a higher propensity to fall for in app purchases upon exposure.

Technological risks

Children are amenable to the use of emerging technologies like Virtual Reality and Artificial intelligence. The privacy risks which they carry are overshadowed by the benefits they accrue. Artificial Intelligence (AI) is largely credited with increasing efficiency of work and minimizing delays through automation. Generative AI relies on a learning model which is possible through creation of a large database. This database helps chatbots to give responses according to the behavioral tendencies of the user. According to UNICEF (2021), children interact with AI through toys, virtual assistants and chatbots [16]. For instance, Hello Barbie, an interactive doll, became a very popular toy among the children. It was later discovered that the doll prompts children to reveal personal information. The

[14] Radesky, J., Chassiakos, Y. (Linda) R., Ameenuddin, N., & Navsaria, D. (2020). Digital Advertising to Children. *Pediatrics*, *146*(1), e20201681. https://doi.org/10.1542/peds.2020-1681

[15] Study on the impact of marketing through social media, online games and mobile applications on children's behaviour

[16] *Digital Child's Play: protecting children from the impacts of AI*. (2021, November 27). UN News. https://news.un.org/en/story/2021/11/1106002

audio recordings of children were stored in not-so-secure servers which had been hacked. The propensity of child surveillance and profiling of their data increases with the use of such technology [17]. Similarly, the harmless appearing Virtual Reality has significant security risks associated with it. It is extensively used by children as a means of simulating reality. Malicious actors can use VR data such as eye movement and hand gestures to create deep fakes and estimate the PIN of a device through gestures.

Legal framework of data protection in India

Social context of privacy in India

Laws are often a product of the social context in which they are placed. The implications of privacy are different in collectivistic and individualistic societies [18]. We can say that Indian society is a collectivistic one with a propensity towards a joint family. There are multiple indices which prove the same. Hofstede used power distance, individualism, masculinity and uncertainty avoidance to come up with an index to measure cultural relativism and cross cultural differences. This index revealed that professional relationships between superior and subordinate resemble the relations between a father and son. The connotations of privacy in a collectivistic society are vastly different from those of individualistic societies of the west . According to a study by Kumarguru et al (2005), respondents in the US associated privacy with the idea of informational privacy while those in India considered physical privacy to be more important. The concern towards data privacy is much lower in India compared to the US [19]. As pointed out by these examples, the understanding of privacy is shaped by culture and is context dependent. In such a context, familial relations are seen as an exception to the privacy of a child. Parental surveillance of children's browsing history and online behavior is considered to be legitimate.

---

[17] Irwin, J., Dharamshi, A., & Zon, N. (2021). *Children's Privacy in the Age of Artificial Intelligence.* https://www.csagroup.org/wp-content/uploads/CSA-Group-Research-Children_s-Privacy-in-the-Age-of-Artificial-Intelligence.pdf

[18] Hofstede, G. (1983). National Cultures in Four Dimensions: A Research-Based Theory of Cultural Differences among Nations. International Studies of Management & Organization, 13(1-2), 46–74.

[19] Kumaraguru, P., Cranor, L., & Newton, E. (n.d.). Privacy Perceptions in India and the United States: An Interview Study. Retrieved August 4, 2024, from https://www.cs.cmu.edu/~ponguru/tprc_2005_pk_lc_en.pdf

Case laws related to privacy in India

Although there is an absence of children's mention in India's privacy jurisprudence. We shall examine the evolving nature of privacy in the Indian legal context. In *Kharak Singh vs State of Uttar Pradesh* [20] and *Govind vs State of Madhya Pradesh* [21], right to privacy, though ambiguous, was considered to be critical in the maintenance of Article 21. The dissenting opinion of Justice Subba Rao in both the cases compared an individual's house as a caste, inside which he ought to be free from encroachments. The domiciliary surveillance encroachments of the Police were considered to be an unreasonable restriction to the privacy of an individual.

The majority ruling in *R Rajagopal vs State of Tamil Nadu* [22] held that privacy was the right to be left alone. An external authority cannot publish details about an individual's family, marriage, procreation, motherhood, child-bearing without the permission of the given individual. The Supreme Court ruled in *PUCL vs Union of India* that the constitution does not recognise the right to privacy in itself. This has two connotations: the right to privacy is not a standalone right neither is it expressly guaranteed in the Indian legal framework. The *Puttaswamy vs Union of India* [23] case recognised the right to privacy as an independent rather than an instrumental right merely meant to protect other rights. The ruling, recognising the right to privacy as an express right did not lay down the contours of the right. The doctrine of proportionality and legitimacy has been laid down in the case to determine state intervention in one's private domain.

[20] 1963 AIR 1295, 1964 SCR (1) 332

[21] 1975 AIR 1378, 1975 SCR (3) 946

[22] 1995 AIR 264, 1994 SCC (6) 632

[23] (2017) 10 SCC 1, AIR 2017 SC 4161

Statutory laws

The Information Technology Act, 2000 [24]was the first iteration of a data protection law in India. However, the emphasis of the act is on the characterisation of cybercrime and the scope of offenses. The act provides legal recognition to e-governance, e-commerce. Chapter IX of the Act defines the punishment for accessing data from secure computer networks or introduces a virus in the network. Chapter XI defines tampering with source documents, publishing obscene images and hacking the computer information as offenses. Section 43A was introduced in 2008 through an amendment, to hold 'body corporate' liable to compensate data subject if the due procedures for data collection are not followed[25]. However, Section 69 empowers the government to decrypt information in the interest of sovereignty and integrity of the nation.

The IT Act was followed by Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[26]. The IT Rules made a distinction between personal information and sensitive personal information. Personal information is defined as information which relates to a natural person, which is likely to be available with a corporate entity. Whereas, sensitive personal information consists of passwords, financial information, biometric information etc [27]. The rules place a bunch of obligations for the corporate entity apart from this: they have to declare the purpose for which information is collected, ensure that the information is processed for the purpose it was collected and it must make sure that its privacy policy is available for public view [28].

[24] Information Technology Act, 2000

[25] Srinivas, Nimisha, & Biswas, Arpita. (2012). Protecting patient information in india: data privacy law and its challenges. NUJS Law Review, 5(3), 411-424.

[26] Information Technology Rules, 2011

[27] Duraiswami, D. R. (2017). Privacy and Data Protection in India. Journal of Law & Cyber Warfare, 6(1), 166–186. http://www.jstor.org/stable/26441284

[28] Duraiswami, D. R. (2017). Privacy and Data Protection in India. Journal of Law & Cyber Warfare, 6(1), 166–186. http://www.jstor.org/stable/26441284

The Digital Data protection Act, 2023[29] is a culmination of the Shrikrishna Committee report and is the primary law which governs data protection in India. It defines data principal as the person whose data is being collected, Data Fiduciary as the authority which determines the purpose of processing data and data processor as an authority which processes the data of individuals. It also introduces a consent manager who enables the principal to manage their consent and withdraw it when they feel so. According to Section 4 of the act, every request for consent of the data principal ought to be in clear and plain language. Consent of the principal must be voluntary and can be withdrawn at any moment. Data principal has the right to erasure, correction, access, grievance redressal and nomination. However, they don't have a right to data portability which deals with the transfer of data from one data fiduciary to another. The Shrikrishna committee report which is the basis of the act does not delve into the rationality of consent which is provided. There is empirical evidence to suggest that less than 10% of the users read the entire privacy agreement. The emphasis on consent clause may lead to more exacerbating of user trust on data fiduciaries without essentially increasing data privacy [30]. Section 7 of the Act mandates that the processing of personal data can only be done for reasonable purposes for which the principal has voluntarily agreed. There are multiple exceptions to this provision: for protecting the sovereignty and integrity of India, during medical emergencies or breakdown of law & order. The use of blockchain for data processing presents a unique set of challenges insofar as there is a lack of a centralized node which stores all data. The act does not necessitate data fiduciaries to create accountability records which refer to details of breaches which have happened and the action taken on them. [31].

The Act, despite provisions pertaining to children, does not identify children as vulnerable stakeholders in the digital space. There is a lack of provisions which protect the digital rights of children. The fiduciaries cannot engage in behavioral monitoring of children or targeted

[29] Digital Data Protection Act, 2023

[30] Burman, A. (2020). Will India's Proposed Data Protection Law Protect Privacy and Promote Growth? https://carnegie-production-assets.s3.amazonaws.com/static/files/Burman_Data_Privacy.pdf

[31] Decrypting India's New Data Protection Law: Key Insights and Lessons Learned

advertisement. Section 9 mandates consent of parents or lawful guardians for the processing of data. There is a lack of description of rights of children or the detrimental practices which can be used by companies to mine the data of children.

Analysis of Data protection laws in EU with respect to Children's rights

Context of child rights in the international sphere

There has been a long standing dilemma between protection and empowerment while coming up with child rights. On the one hand, those advocating for protection argue that children don't have decision making autonomy. The need for protection of children was recognised through the UNCRC [32] and Oslo challenge[33]. Their rights are at the behest of their parents. The welfarist model of evaluation of the child's best interest rests with the parents. Children are seen to be devoid of the ability to make claims in order to impose duties on others. On the other hand, advocates of empowerment postulate that their decision making power is seen to be independent of influence. Such a conception of rights vows a child as a moral agent who can make claims for their rights [34]. CRC rules that consent is important for photography and dissemination, it is a control right which includes the right to refuse to be clicked. Article 16 of the convention requires that state parties must take measures to protect their information from non state actors. There is an attempt to balance the right to privacy with the right to freedom of expression. It also mandates states to come up with effective data protection laws in order to check any unlawful interference with the privacy of children [35].

Bright line rule followed in western democracies determines an inflexible age which suits legislative purpose. The bright line rule implies that 13 years is a threshold age above which an individual is no longer considered to be a child. The rule ignores the reality that mental and cognitive capacities of

[32] https://www.unicef.org.uk/wp-content/uploads/2016/08/unicef-convention-rights-child-uncrc.pdf

[33] https://archive.crin.org/en/docs/oslo.pdf

[34] EEKELAAR, J. (1992). THE IMPORTANCE OF THINKING THAT CHILDREN HAVE RIGHTS. "International Journal of Law, Policy and the Family," 6(1), 221–235. https://doi.org/10.1093/lawfam/6.1.221

[35] Monitoring State Compliance with the UN Convention on the Rights of the Child. (2022). In Z. Vaghri, J. Zermatten, G. Lansdown, & R. Ruggiero (Eds.), Children's Well-Being: Indicators and Research. Springer International Publishing. https://doi.org/10.1007/978-3-030-84647-3

every child evolves at a different pace[36]. The inflexible age limit undermines an underage child's ability to consent despite attaining maturity. Though the idea of consent itself can be problematised as in today's digital world, there is only a nominal choice between accepting terms and conditions or abandoning the use of the application in itself [37]. Social media applications often contain very long and heavily worded privacy conditions which are incomprehensible to children. A consequence of the same is that they are unable to understand them in the first place. Even if they understand and decide to decline them, they will be forced to terminate the usage of the given application [38].

General Data Protection Regulation Law

The European Union's General Data Protection Regulation (GDPR) [39]devotes special attention to the personal data of children. Previous data protection laws were agnostic to age, data controllers were supposed to abide by a standard set of regulations for personal data. The inclusion of children was due to their lack of awareness of the consequences of data compromise which makes them vulnerable to malicious data extraction.

Article 8 deals with the processing of data pertaining to children. Consent of children can only be considered to be legitimate if they acquire the age of 16. A common critique of the law is that the threshold age is too high, denying the opportunity to those children who consent to data processing but have not reached the age to consent. The law follows a graduated approach in which a child's capacity to consent increases with age. If a data subject (an individual whose data is to be collected) is under the threshold age, the data controller (the entity which is responsible for collection of data) ought to ensure that the consent is provided by a legitimate parental authority. The act also guarantees the right to be forgotten, which implies that children can revoke their consent for parting with

[36] Macenaite, M. (2017). From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. New Media & Society, 19(5), 765–779. https://doi.org/10.1177/1461444816686327

[37] Donovan, S. (2020). "Sharenting": The Forgotten Children of the GDPR. Peace Human Rights Governance, 4(1), 35–59. https://doi.org/10.14658/pupj-phrg-2020-1-2

[38] Jasmontaite, L., & De Hert, P. (2014). The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet. *International Data Privacy Law*, *5*(1), 20–33. https://doi.org/10.1093/idpl/ipu029

[39]General Data Protection Regulation (GDPR)

personal information at a later stage. This is called the right to erasure and can be found in Article 17 of the law.

The issue of sharenting arises with respect to parental role as a gatekeeper of their children's information. **Sharenting** involves use of social media by parents to share minute details of their children's lives without their consent. The act mandates verification of consent without establishing any mechanism to enforce the same. This poses two interconnected issues: How can one verify if a child is over the default age of consent and if the child is not, how to verify if consent is provided by a legitimate parental authority. Usually, social networking websites set up a minimum age limit, there is an absence of any mechanism to check the legitimacy of the age which is being entered. The mechanism relies on self certification or a declaration by the user confirming her age to be above the threshold. According to a survey conducted in the USA, 68% of pre-teens had access to social media. 47 % and 31% of children aged between 11 and 12 used TikTok and Snapchat respectively. This is notwithstanding the fact that both the applications have a minimum age limit of 13 years [40].

Ambiguous definitions in the act

Section 6(1) of GDPR provides a lawful basis for the data processing by information society services offered directly to a child. Information society services are services provided for remuneration upon the individual request of the recipient. Going by this definition, a majority of services including search engines, video games and music can be considered to be ISS. It is unsure if services offered by not for profit or educational organizations fall within the scope of this article. Services offered directly to children have not been defined in the act. The case of Youtube is a classic example of this dilemma. If we evaluate the article at its word, then only Youtube Kids will fall within the scope of this act. Using such a narrow definition implies that content which is consumed by children on Youtube will not be cognisable under the provisions of this act [41].

---

[40] Dixon, S. J. (2023, December 4). *U.S. pre-teen social media reach 2022*. Statista. https://www.statista.com/statistics/1417175/us-preteens-social-media-reach/

[41] Ruzgar, S., Caglar, Y., & Caglar, M. (2021). The optoelectrical properties of rare earth element Eu doped CuxO based heterojunction photodiode. *Chinese Journal of Physics*, *72*, 587–597. https://doi.org/10.1016/j.cjph.2021.05.017

Article 6 (1)(f) provides a balancing test: A data controller can only process data if it is in its legitimate interest, processing of data cannot happen if the legitimate interest of the controller conflicts with the fundamental rights of a child. In these provisions, legitimate purposes have not been defined. For a marketing firm, advertisement may be considered to be a legitimate purpose but it may be in contravention of the rights of data subjects [42]. The Information Commissioner's Office places an obligation on the data controller to be charitable in arriving at an understanding of legitimate interest. Following factors must be taken into account while developing a conception of legitimate interest: age range of the children, Data protection and access of children to the service [43].

Recommendations to strengthen India's data protection framework

1. Defining Best/Detrimental interests of the child

The Indian Data protection law must include a comprehensive definition of the best interests of the child. Worldwide, the conception of best interest has been the guiding force behind data protection laws. Determination of best interests of children depends on two interrelated factors: relationship between data controllers & data subjects and standards for processing data. Best interest of children is attained when they are placed at an equal footing with the commercial data collectors. Framing the best interest of children in a policy framework will act as a guiding force for data collectors as to when they should or should not collect data. Enunciation of best interest of children has two tangible benefits: it defines the space for participation, experimentation and social engagement (spatial autonomy) and it brings out a distinction between their traditional conception of autonomy & autonomy in the digital world (informational autonomy)[44]. Best interest of children can either be defined positively in terms of

[42] *The General Data Protection Regulation and children's rights: questions and answers for legislators, DPAs, industry, education, stakeholders and civil society Roundtable Report*. (2017). https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf

[43] *The General Data Protection Regulation Children and the GDPR*. (2018). https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf

[44] Savirimuthu, J. (2019). Datafication as parenthesis: reconceptualising the best interests of the child principle in data protection law. International Review of Law, Computers & Technology, 1–32. https://doi.org/10.1080/13600869.2019.1590926

what they are or negatively in terms of what they are not. The child's view, identity, preservation of family environment, situational vulnerability, right to health and education are key factors highlighted by UN Committee on rights of child to determine the best interest of the child [45]. The Age Appropriate design code[46] (the Data protection law in the United Kingdom) categorizes detrimental use of data into: Marketing and behavioral advertising, broadcasting, press and online games .

2. Establishment of Digital Data Protection Board

India's Digital Data Protection Act mandates the formation of a digital data protection board. Chapter V governs the working of the board, which has not been formed since the passage of the law. The chairperson of the board shall be appointed by the Union government. The board has the power to impose a penalty in case of a data breach and determine grounds for inquiry. However, the board must have a more decentralized approach with nodal boards established at the state level. This will help in dealing with data breaches at two levels: union and state. The board also must reveal a monthly report on state wise data breaches and an Action Taken Report. This will enable greater transparency and competitive federalism as the states will try to outpace each other in improving their data protection framework. It will also ensure transparency in as much as the data subjects will be aware about whether the data compromised has been recovered and whether a penalty has been imposed on the data controller. The Digital Data Protection Board must include appointment of Children's Data Protection Officers (CDPO). These officers will particularly look at the data protection for children. CDPOs will play a key role in preparing the data compliance report. Their presence will ensure greater accountability in the process of safeguarding children's digital rights as they can be held directly responsible for the same. The CDPOs must be part of a permanent wing within the board to regulate children's data protection exclusively.

---

[45] Fundamentals of Child Oriented Data Processing

[46] Age Appropriate Design Code

3. Privacy Impact Assessment

Indian data protection acts allow for processing of data for a variety of subjects, it does not mandate carrying out an impact assessment prior to processing of the data Privacy impact assessment is carried in order to ensure 'privacy by design.' Projection of high risks to rights of children through assessment will compel the commercial interest to alter the nature of processing so as to mitigate the privacy harm. A critique offered against mandating PIA is that it may become a statutory exercise with a motivation to escape penalisation rather than a creative one [47]. According to the CPRA,[48] The California Privacy Protection Agency is responsible for conducting regular risk assessments to weigh the costs and benefits of data processing to the children and data controller. As part of a child centric approach, the Data protection authority should conduct regular Child Rights Impact Assessments. CRIA is an empirical mechanism to ensure that the best interests of children are being represented. The Dutch code (Data protection law of The Netherlands)[49] came up with a two step process to maintain the robustness of the process. In the assessment stage, all factors relevant to the interest of the children are charted down. The second stage is the determination stage where the data controllers are held accountable for the protection of interest of children .

'Privacy by design' and 'privacy by default' refers to the integration of data protection mechanisms into product development [50]. If the data subjects are offered a choice to opt into the privacy policy, the default option must be the most privacy friendly ones. The default privacy policy must rely on a model which mandates only the collection of essential cookies. The concepts of data minimization and purposeful collection are closely linked to privacy by default[51]. The lesser amount of data there is with the data collector, the lesser are chances of a breach/misuse of data. The Irish Fundamentals of a child oriented data processing uses the bake it in approach to embed privacy in product designs. The dutch

---

[47] Binns, R. (2017). Data protection impact assessments: a meta-regulatory approach. International Data Privacy Law, 7(1), 22–35. https://doi.org/10.1093/idpl/ipw027

[48] California Privacy Rights Act, 2020

[49] Dutch Code

[50] https://www.emerald.com/insight/content/doi/10.1108/JICES-10-2014-0040/full/html?skipTracking=true

[51] Willis, L. E. (2014). Why not privacy by default?. *Berkeley Technology Law Journal, 29(1),* 61-134.

code includes the following compliance rules: individual selection of every form of optional data collection; geolocation, microphone and camera settings denied by default and display of warning if the child tries to change the privacy settings.

5. Age Verification mechanisms

Current data framework relies on the self certification of children's age. There is no mechanism to check whether the age entered by the children is accurate or not. The logical outcome of such a provision is that it leads to underage children being able to create social media accounts. Document based verification is an alternate provision which can be used by social media platforms. This provision requires children to upload a government recognised identity card before creating an account on any social media platform. This testifies the authenticity of consent provided by the child.

6. Regulation of Targeted Advertising

There should be a blanket ban on all forms of behavioral and surrogate advertising. Surrogate advertising results in association of a brand name with relatively harmless products. This is despite the fact that the primary product of that brand might be harmful in nature. Such advertisements targeted towards children can manipulate their consumption choices. The advertisements in games must be clearly labeled, this ensures transparency and prevention of deceptive practices. Proper disclaimers should be given in lucid language regarding the purpose of data collection.

7. International Framework for children's data protection

India's data protection policy must align with the principles and practices established in the GDPR , which is considered to be the globally accepted standard for data protection. The framework of rights of children should not be in contravention of the UNCRC. There should be transnational cooperation between India's Data Protection Authority with that of other authorities in order to enhance sharing of technology and common threats. The Act must also impose stringent conditions on cross border transfer of children's data. This can be ensured by maintaining a parity with data

protection laws worldwide. This prevents hackers with malicious intent from exploiting the loopholes in data protection law of India. Strong penalties must be imposed to all violators of data protection. The potential violators can be state or non state actors. To punish state actors, the board must be given constitutional rather than statutory authority. This will guarantee financial autonomy and lack of dependance on the government. The ultimate goal is to establish the board as a neutral watchdog for children's data protection concerns.

Conclusion

Data protection in India fails to address the unique challenges associated with processing of children's data. Given that they are more vulnerable to data compromise, it is in their interest that the government takes measures to protect their data. There is a need to strengthen the institutional structure and make laws more stringent in the incidence of data breaches. Companies must be held accountable not just to the data protection board but also to the citizens. Consent of children needs to be managed in a more nuanced manner. They need to be given the right to erasure and withdrawal of their consent at a later stage of their childhood/adulthood.

References

Agarwal, V. (2012). Privacy and data protection laws in India. *International Journal of Liability and Scientific Enquiry*, *5*(3/4), 205. https://doi.org/10.1504/ijlse.2012.051949

Binns, R. (2017). Data protection impact assessments: a meta-regulatory approach. *International Data Privacy Law*, *7*(1), 22–35. https://doi.org/10.1093/idpl/ipw027

Brown, D. H., & Pecora, N. (2014). Online Data Privacy as a Children's Media Right: Toward Global Policy Principles. *Journal of Children and Media*, *8*(2), 201–207. https://doi.org/10.1080/17482798.2014.893756

Burman, A. (2020). *Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?* https://carnegie-production-assets.s3.amazonaws.com/static/files/Burman_Data_Privacy.pdf

California Privacy Rights Act. (2020). Thecpra.org. https://thecpra.org/

CHILDREN FRONT AND CENTRE FOR A CHILD-ORIENTED APPROACH TO DATA PROCESSING FUNDAMENTALS. (2021). https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf

Dias, P., Brito, R., Ribbens, W., Daniela, L., Rubene, Z., Dreier, M., Gemo, M., Di Gioia, R., & Chaudron, S. (2016). The role of parents in the engagement of young children with digital technologies: Exploring tensions between rights of access and protection, from "Gatekeepers" to "Scaffolders." *Global Studies of Childhood*, *6*(4), 414–427. https://doi.org/10.1177/2043610616676024

Digital Child's Play: protecting children from the impacts of AI. (2021, November 27). UN News. https://news.un.org/en/story/2021/11/1106002

Dixon, S. J. (2023, December 4). *U.S. pre-teen social media reach 2022*. Statista. https://www.statista.com/statistics/1417175/us-preteens-social-media-reach/

Donovan, S. (2020). "Sharenting": The Forgotten Children of the GDPR. *Peace Human Rights Governance*, *4*(1), 35–59. https://doi.org/10.14658/pupj-phrg-2020-1-2

EEKELAAR, J. (1992). THE IMPORTANCE OF THINKING THAT CHILDREN HAVE RIGHTS. *"International Journal of Law, Policy and the Family," 6*(1), 221–235. https://doi.org/10.1093/lawfam/6.1.221

Elliott, V. (2023). *A Major App Flaw Exposed the Data of Millions of Indian Students*. Wired. https://www.wired.com/story/diksha-india-education-app-data-exposure/

European council. (2022, September 1). *The general data protection regulation*. Www.consilium.europa.eu. https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/#:~:text=data%20protection%20rules-

Government of India. (2023, August 11). *Ministry of Electronics and Information Technology, Government of India | Home Page*. Www.meity.gov.in. https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

Hofstede, G. (1983). National Cultures in Four Dimensions: A Research-Based Theory of Cultural Differences among Nations. *International Studies of Management & Organization*, *13*(1-2), 46–74.

Hye Jung Han. (2022, May 25). *"How Dare They Peep into My Private Life?"* Human Rights Watch. https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments#_ftn82

Information Technology Act. (2000). https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=

Irwin, J., Dharamshi, A., & Zon, N. (2021). *Children's Privacy in the Age of Artificial Intelligence*. https://www.csagroup.org/wp-content/uploads/CSA-Group-Research-Children_s-Privacy-in-the-Age-of-Artificial-Intelligence.pdf

Jasmontaite, L., & De Hert, P. (2014). The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet. *International Data Privacy Law*, *5*(1), 20–33. https://doi.org/10.1093/idpl/ipu029

Kumaraguru, P., Cranor, L., & Newton, E. (n.d.). *Privacy Perceptions in India and the United States: An Interview Study*. Retrieved August 4, 2024, from https://www.cs.cmu.edu/~ponguru/tprc_2005_pk_lc_en.pdf

Livingstone, S., & Bulger, M. (2014). A Global Research Agenda for Children's Rights in the Digital Age. *Journal of Children and Media*, *8*(4), 317–335. https://doi.org/10.1080/17482798.2014.961496

Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). *Children's Data and Privacy Online Growing up in a Digital Age an Evidence Review*. https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf

Macenaite, M. (2017). From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. *New Media & Society*, *19*(5), 765–779. https://doi.org/10.1177/1461444816686327

McCloskey, H. J. (1980). Privacy and the Right to Privacy. *Philosophy*, *55*(211), 17–38. https://doi.org/10.1017/s0031819100063725

Monitoring State Compliance with the UN Convention on the Rights of the Child. (2022). In Z. Vaghri, J. Zermatten, G. Lansdown, & R. Ruggiero (Eds.), *Children's Well-Being: Indicators and Research*. Springer International Publishing. https://doi.org/10.1007/978-3-030-84647-3

Moor, J. H. (1997). Towards a theory of privacy in the information age. *ACM SIGCAS Computers and Society*, *27*(3), 27–32. https://doi.org/10.1145/270858.270866

Nissenbaum, H. (1997). Toward an Approach to Privacy in Public: Challenges of Information Technology. *Ethics & Behavior*, *7*(3), 207–219. https://doi.org/10.1207/s15327019eb0703_3

O'NEILL, O. (1992). CHILDREN'S RIGHTS AND CHILDREN'S LIVES. *"International Journal of Law, Policy and the Family," 6*(1), 24–42. https://doi.org/10.1093/lawfam/6.1.24

Online learning products enabled Surveillance of children . (2024). Hrw.org. https://www.hrw.org/news/2022/07/12/online-learning-products-enabled-surveillance-children#:~:text=Human%20Rights%20Watch%20released%20technical

Radesky, J., Chassiakos, Y. (Linda) R., Ameenuddin, N., & Navsaria, D. (2020). Digital Advertising to Children. *Pediatrics*, *146*(1), e20201681. https://doi.org/10.1542/peds.2020-1681

Ruzgar, S., Caglar, Y., & Caglar, M. (2021). The optoelectrical properties of rare earth element Eu doped CuxO based heterojunction photodiode. *Chinese Journal of Physics*, *72*, 587–597. https://doi.org/10.1016/j.cjph.2021.05.017

Savirimuthu, J. (2019). Datafication as parenthesis: reconceptualising the best interests of the child principle in data protection law. *International Review of Law, Computers & Technology*, 1–32. https://doi.org/10.1080/13600869.2019.1590926

TAVANI, H. T. (2007). PHILOSOPHICAL THEORIES OF PRIVACY: IMPLICATIONS FOR AN ADEQUATE ONLINE PRIVACY POLICY. *Metaphilosophy*, *38*(1), 1–22. https://doi.org/10.1111/j.1467-9973.2006.00474.x

The General Data Protection Regulation and children's rights: questions and answers for legislators, DPAs, industry, education, stakeholders and civil society Roundtable Report. (2017). https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf

The General Data Protection Regulation Children and the GDPR. (2018). https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf

The Handbook of Information and Computer Ethics. (2008). https://doi.org/10.1002/9780470281819

The Protection of Children Online. (2011). *OECD Digital Economy Papers*. https://doi.org/10.1787/5kgcjf71pl28-en

Thomson, J. J. (1975). The Right to Privacy. *Philosophy & Public Affairs*, *4*(4), 295–314. https://www.jstor.org/stable/2265075