
SAFE FROM WHOM? THE PRICE OF PROTECTING CHILDREN ONLINE

Bibhanshu Baibhav, B.A.LL.B. (Hons.), UILS, Chandigarh University, Punjab

ABSTRACT

The rise in the dangers of online manipulation and abuse and exposure to unsuitable material has made the debate around the protection of children in cyberspace an important one. But while methods that guarantee the online safety of children can themselves be at odds with children's constitutional rights of free speech, access to information, and privacy, the objective of such regulations remains. In this essay, the constitutional issues around restrictions of children's internet usage will be explored, with focus specifically on the judgment in *Just Rights for Children Alliance v. S. Harish* and the principle of proportionality in *K.S. Puttaswamy v. Union of India*. At the same time, privacy implications of the age verification systems and parent consent under Section 9 of the Digital Personal Data Protection Act, 2023 will be considered as well. The goal here will be to demonstrate that, far from being always the most effective measure in the protection of children in cyberspace, outright bans might limit children's access to learning and information too much. The need instead would be for a rights-focused system of protection, which involves data minimization, proper privacy settings according to age, prevention of contact by unsolicited persons, strong content regulation and easy-to-access channels for reporting.

The internet can expose children to exploitation, abuse and inappropriate material. However, even while safeguarding children against these threats, a tough constitutional problem arises: up to what point can the state limit their online lives for the sake of security?

According to the October 15, 2026, decision made by the Supreme Court in the case of *Just Right for Children Alliance V. S. Harish*¹, the right to use and access the internet was considered a basic right enshrined under Articles 19(1)(a) and 21² of the Constitution of India. This court refused to support blanket bans on internet access to children since it considers that the restrictions should be directed at offensive material and people responsible for it, and not the children themselves, at least in theory. In its approach to protecting children from the internet, the court recognises the conflict between protection of children and freedom.

It is not about compromising the safety of children versus their freedom but making sure that the two are not compromised unreasonably for each other's sake.

THE CONSTITUTIONAL FOUNDATION

The importance of the Supreme Court judgement from the constitutional point lies in acknowledging that children are rights holders, and not merely individuals whose digital lives can be understood completely by adults, in general. In the case of *Just Rights for Children Alliance v. S. Harish*³, the Supreme Court held that the access and usage of the internet is a fundamental right, which is protected by Articles 19(1)(a) and 21 of the Constitution, irrespective of age. The Supreme Court acknowledged the fundamental right to access the internet by children due to its role in education and free expression.

But this does not mean that children should be subjected to all kinds of Internet content without any safeguard measures, or at best, the issue from the Constitutional perspective is how a limitation could be justified in terms of its objective and would involve interfering with fundamental rights no more than is necessary in general; in other words, as the Court recognised in the case of *K.S. Puttaswamy V. Union of India*⁴, the Supreme Court ruled privacy is a fundamental right, and legality, legitimacy of objectives, and proportionality are the guiding principles when the state infringes on privacy, among others. The test of proportionality in the

¹ *Just Rights for Children Alliance & Anr. v. S. Harish & Ors.*, 2026 INSC 1149

² INDIA CONST. arts. 19(1)(a), 21.

³ *Just Rights for Children Alliance & Anr. v. S. Harish & Ors.*, 2026 INSC 1149

⁴ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

right to privacy is thus relevant while reviewing digital-safety measures involving the sharing of personal information.

Protecting children is the motive here, but not to the extent that they lose the chance to learn and communicate about life in realistic situations. It is critical to know that the act of detaining is the crucial point because although the act was put in place with the sole purpose for the prevention of any kind of exploitation, it can be deemed as being extreme because it excludes children from rightful areas online.

THE PRIVACY COST OF AGE VERIFICATION

However, verification could require use of platforms for processing of identity papers or age-relevant information as well as parental information, putting forth the question of how much personal data should be required merely to use some online services. Age verification seems to serve as a simple solution to the problem, such as identifying underage individuals and limiting their exposure to inappropriate content. However, age verification itself could become another obstacle.

There are also the regulations concerning verifiable parental consent as far as processing personal data of children in the Digital Personal Data Protection Act, 2023, of India is concerned. Section 9⁵ of the Act provides that verifiable parental consent will have to be obtained before processing personal data of a child, except where there are exceptions from the Act.

The problem is that surveillance and verification are two different concepts, because the verification process does not necessarily require collecting any detailed information regarding a user's identity as well as his activities; usually, however, this is not the case. The difference is important considering that such system is used to collect information both from adults and children and hence putting both of them at risk of excessive collection of information, at least empirically. There is another issue connected with function creep, according to which information gathered for age verification can be then used for other purposes; also, centralised identity records might be exposed to data breaches. All of these factors explain why regulation should consider whether age verification is necessary as well as what should be done with the

⁵ Digital Personal Data Protection Act, No. 22 of 2023, § 9 (India)

resulting information.

Issues regarding age-gating and consent of the parents are in effect demonstrating the importance of setup; consequently, it is possible in practice for barriers to emerge for families with limited access to technology based on a verification system which relies on identity documentation or complicated parental process.

However, it is not about forbidding verification. It should be more about insisting on guards that would match the level of risk in practice and the protection of children from harm must not turn into an excuse for indiscriminate gathering of information about people. In fact, the platform must only collect what is necessary for the purpose.

PROPORTIONALITY, NOT PROHIBITION

The issue here from the view of the constitution is not whether children require any protection in the Internet sphere, it is whether restricting their access to it is the best way to protect them. Such a blanket restriction can be seen as convenient in an administrative sense. However, such an approach views the access as the problem.

The Supreme Court acknowledged the necessity of protection and yet declined to impose any blanket ban on access to the internet for children in case of *Just Right for Children Alliance V. S. Harish*⁶; it demonstrated some suggestions ranging from the establishment of a private account setting, limiting access to message from adults who are not known to the child, to parents' guidance and improved moderations of contents that are available to children to a large extent. Such suggestions hint a much more concentrated approach as eliminating risks while not excluding children from the internet at all for the moment being.

The concept of proportionality requires to explore whether a certain policy is capable of striving its stated objective in general; the use of restrictions for service providers and content that is inherently damaging to children to some degree may be justified under law when properly applied. If it is possible to use privacy measures, restrictions on unsolicited contact, proper complaint systems, and the quick removal of illegal content to address a particular problem, it becomes necessary to find better reasons to use access restrictions.

⁶ *Just Rights for Children Alliance & Anr. v. S. Harish & Ors.*, 2026 INSC 1149

It takes a step back from preventing children from engaging with the digital realm to making the digital world safe, and putting responsibility on the platform for developing such protective measures instead of making it the burden of the children and their parents in the real world; after all, the aim here is to protect without any unreasonable restrictions on their constitutional rights.

A RIGHTS-BASED SAFETY MODEL

A rights-based approach should put the burden of prevention of harm online on those individuals who are most well-suited for the task in practice. Age-appropriate privacy settings should be in use, there should be restrictions on any unwanted contact from adult strangers, there should be a reporting system, which responds to any form of exploitation or illegal material posted.

Age verification, whenever necessary, must follow the principles of data minimization and purpose failure. In fact, the data associated with age verification must be made secure from any form of abuse, age verification should not require platforms to maintain identity documents and collect additional data if that is not actually needed and users must be clearly informed about the information being collected, the purpose behind the collection, and the retention period. An independent evaluation of these frameworks might reveal whether these safeguards work in reality.

Parents play an important role, although it should not lead to complete surveillance of the digital world of the child. While appropriate protection is what children need from parents, the ability to learn and communicate and to build independence at least theoretically needs to remain intact. The means of protecting children should be taken into consideration their evolving capabilities, rather than viewing all children as one homogeneous group. Moreover, there will also be a need to consider those children who do not have appropriate identification documents, devices and adequate parental assistance, otherwise they may find themselves unable to use the necessary information resources, which will be behind difficult verification mechanisms.

Children must be kept safe online yet at the same time they also need to have their constitutional

rights protected; it's not whether the rules that are made are basic when preventing children from accessing the internet, but what matters more in practice is how basic the rules are in ensuring the safety of the internet from them.