

NEEDED, A NEW APPROACH TO DATA PROTECTION FOR MINORS

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

To enjoy additional benefits

CONNECT WITH US

January 24, 2023 12:08 am | Updated 09:29 am IST

COMMENTS

SHARE

READ LATER

'We should not put the onus of keeping our young safe only on parents, but instead it should make it a society-wide obligation' | Photo Credit: Getty Images/iStockphoto

How freely should Indian teenagers access the Internet? And what responsibilities do platforms have towards their minor users? These are important questions to answer correctly to achieve India's digital ambitions. The draft Digital Personal Data Protection (DPDP) Bill, 2022 currently provides for mandatory parental consent for all data processing activities by children, defined as any person aged under 18 years. This approach however misses the mark on two fronts.

First, instead of incentivising online platforms to proactively build safer and better services for minors, the Bill relies on parents to grant consent on behalf of the child in all cases. In a country with low digital literacy, where parents in fact often rely on their children (who are digital natives) to help them navigate the Internet, this is an ineffective approach to keep children safe online.

Second, it does not take into account the "best interests of the child", a standard originating in the Convention on the Rights of the Child, 1989, to which India is a signatory. India has upheld this standard in laws such as the Commissions for Protection of Child Rights Act, 2005, the Right of Children to Free and Compulsory Education Act, 2009, and the Protection of Children from Sexual Offences Act, 2012. However, it has not been applied to the issue of data protection. The Bill does not factor in how teenagers use various Internet platforms for self-expression and personal development and how central it is to the experience of adolescents these days. From taking music lessons to preparing for examinations to forming communities with people of similar worldviews, the Internet is a window to the world. While the Bill does allow the government to provide exemptions in the future from strict parental consent requirements, profiling, tracking prohibitions, etc., this whitelisting process does not acknowledge the blurring lines between what a platform can be used for. For example, Instagram is, strictly speaking, a social media platform, but is regularly used as an educational and professional development tool by millions of artists around the world.

Another issue in the current draft of the DPDP Bill is that each platform will have to obtain 'verifiable parental consent' in the case of minors. This provision, if enforced strictly, can change the nature of the Internet as we know it. Since it is not possible to tell if the user is a minor without confirming their age, platforms will have to verify the age of every user. The government will prescribe later whether verifiability will be based on ID-proof, or facial recognition, or

reference-based verification, or some other means.

Whatever form verifiability takes, all platforms will have to now manage significantly more personal data than before, and citizens will be at greater risk of harms such as data breaches, identity thefts, etc.

Thus we need to shift our approach with respect to children's data before this Bill is brought to Parliament. To avoid the folly of treating unequals equally and blocking off access to the Internet for teenagers these steps are needed.

First, we should move from a blanket ban on tracking, monitoring, etc. and adopt a risk-based approach to platform obligations. Platforms should be mandated to undertake a risk assessment for minors and not only perform age-verification-related corresponding obligations but also design services with default settings and features that protect children from harm. This approach will bring in an element of co-regulation, by creating incentives for platforms to design better products for children.

Second, we need to relax the age of mandatory parental consent for all services to 13 years in line with many other jurisdictions around the world. By relaxing consent requirements, we will minimise data collection, which is one of the principles that the Bill is built on. This relaxation in age of consent in tandem with the risk mitigation approach elucidated above will achieve protection for children online while allowing them access.

This solution draws on the experience and deliberations in the United Kingdom, and in the United States (California, New York, etc.) where age appropriate design codes have been introduced. To tailor this solution to the Indian context, the government should also conduct large-scale surveys of both children and parents to find out more about their online habits, digital literacy, preferences and attitudes.

We must design a policy in India that balances the safety and the agency of children online. We should not put the onus of keeping our young safe only on parents, but instead it should make it a society-wide obligation. We have to get this part of the data protection framework right as India's 'techade' cannot be realised without its young.

Aparajita Bharti is a Founding Partner at TQH, a public policy consulting firm in Delhi. Nikhil Iyer is a Senior Analyst at TQH, a public policy consulting firm in Delhi

COMMENTS

SHARE

[internet](#) / [children](#) / [data protection](#) / [media](#) / [laws](#) / [parent and child](#)

BACK TO TOP

Comments have to be in English, and in full sentences. They cannot be abusive or personal. Please abide by our [community guidelines](#) for posting your comments.

We have migrated to a new commenting platform. If you are already a registered user of The Hindu and logged in, you may continue to engage with our articles. If you do not have an account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.

END

Downloaded from crackIAS.com

© **Zuccess App** by crackIAS.com

CrackIAS.com