Economic Analysis of Verifiable Parental Consent Mechanisms

Key Findings

The Digital Personal Data Protection (DPDP) Act, 2023, emphasises on individual consent, enhancing user control over personal data. It includes specific protections for children under 18, with Section 9 mandating data fiduciaries to obtain verifiable parental consent (VPC) from parents of the child. The recently released draft DPDP Rules propose that data fiduciaries verify parental identity and obtain parent's consent and propose two methods. 1) using existing platform data for current users, 2) through government-authorised entities or virtual non-user tokens.

This report analyses these proposed and other methods available for obtaining VPC and aims to present frameworks for policymakers and platforms to foster innovation while ensuring child safety and data protection. While regulatory intent is legitimate, factors such as parental digital literacy, privacy, security, and the financial costs of implementing VPC must be carefully considered.

VPC implementation costs are significant, involving expenses such as recurring software subscriptions, staff training, data collection, storage, and ongoing verification. Estimates from other countries, such as the U.S., suggest initial infrastructure costs of around $35,000 and ongoing annual costs of $70,000–$120,000.[1] Given that 29.9% of internet users are aged 0–17,[2] mandatory VPC systems could significantly impact a wide range of digital services, particularly those designed for children, making affordability and feasibility key concerns.[3]

The analysis of various VPC methods highlights that the DPDP draft Rules' prescribed verification mechanisms—using existing platform data or government-authorised services like Digital Locker—may not be optimal in terms of security, cost, or efficiency. More flexible alternatives could enhance security for both minors and parents while reducing operational burdens.

[1] https://www.govinfo.gov/content/pkg/CHRG-106hhrg67635/pdf/CHRG-106hhrg67635.pdf
[2] https://datareportal.com/reports/digital-2024-india
[3] https://www.youthkiawaaz.com/dpdpsurvey/

No single verification method is accurate across all key parameters—cost, privacy, convenience, accuracy, and scalability. Some methods, like self-declaration and SMS consent, are cost-effective and scalable but lack accuracy and robustness, making them suitable for low-risk scenarios. Conversely, methods such as government ID verification or video consent offer higher accuracy but can be costly and inconvenient, making them more appropriate for high-risk contexts.

Estimated Costs of different methods (for 1,000,000 annual verifications)[4]

Method	Infrastructure/ Setup Cost (A)	Operational Costs (B)	Storage Costs (C)[5]	Total Cost (A +B +C)	Total Cost (Average)	Cost Scale (Low To High)[6]
Self Declaration	10,000	818 – 996	260	11,078 – 11,256	11,167	Low
Age Estimation (AI/ML)	7,800	494,618[7]	260	502,678	502,678	High
Government-Issued ID	10,000	5,882 –176,471	260	16,148 – 186731	101,440	Medium
DigiLocker	10,000	35,176	260	45,436	45,436	Low
Credit cards	10,000	5,294	260	15,554	15,554	Low
KBA	10,000	800,000	260	810,260	810,260	High
Third-Party Verification	10,000	235,294[8]	260	245,554	245,554	Medium
Email based consent	10,000	1,506 –10,864	260	11,766 – 21,124	16,445	Low
Video consent	10,000	1,294 – 67,059	23,852[9]	35,416 – 100,911	68,164	Medium
SMS based consent	10,000	1,941	260	12,201	12,201	Low
ZKP	23,640	26,588	260	50,458	50,458	Medium
Operating System/ App store	25[10]	1,764 – 3,727[11]	260	2049 – 4012	3,031	Low
Interoperable VPC	10,000	Shared between platforms	260	10,260	10,260	Low

4 All the costs are in US$ and rounded off

5 For simplicity, US$260, the average storage cost discussed above, has been taken.

6 **Low**: Below US$50,000, **Medium**: Between US$50,000 and US$500,000, **High**: Above US$500,000.

7 US$494,118 for annual 1,000,000 verifications and average annual subscription fees of US$500.

8 The cost has been calculated based on a single verification, but service providers have indicated that it will decrease significantly as the user base grows. However, the exact amount can only be determined once the Rules come into effect.

9 The average storage costs for the video file discussed above have been taken.

10 for Google Play Store.

11 Includes US$99 annual fee for Apple.

Key Features of different methods

Method	Privacy	Convenience	Accuracy	Scalability
Self Declaration	High because of minimal data collection	High because of its simplicity and accessibility	Very low due to lack of proof and potential for manipulation	Highly effective for low-risk use cases and on a larger scale
Age Estimation (AI/ML)	Low, due to continuous data collection and monitoring	High, as users may not be even aware	Moderate but prone to errors for near-age thresholds (e.g. 17 & 18)	Moderately scalable
Government-Issued ID	Low because of the risk of exposure to sensitive data	Low because it is time-consuming and can exclude users without official IDs	High accuracy when implemented with additional checks	Low, difficult to scale, especially in resource-constrained areas and populations without IDs
DigiLocker	Low, because of the potential to reveal other details like name	Low, because of limited penetration	High as Aadhaar KYC is already used in the financial sector	Moderate because DigiLocker may not have universal access
Credit cards	Low, as limited threat of exposure of sensitive financial data	Moderate, as it is simple but excludes families without access to cards	Moderate, has risks in case of children having access to joint cards	Low due to limited card penetration in countries like India
Knowledge Based Assessment	Moderate to high privacy risks if knowledge about personal data is assessed	Moderate and hardware-free, but users may face frustration due to a set of personal questions	Moderate since it is vulnerable to generic or inaccurate answers	Low, costly and challenging to scale
Third-Party Verification	Low privacy & potential data overexposure to external entities	High convenience but requires trust in third-party services	High but varies with implementation quality	Medium scalability but resource-intensive
Email based consent	High, collects limited data but is vulnerable to spoofing	High, easy to implement, relies on a common communication method	Low due to susceptibility to circumvention by tech-savvy minors	Moderate as it can scale efficiently with optimised delivery systems; but assumption is widespread email access
Video consent	High privacy risk from facial and identity data	Low as it requires digital literacy and is invasive, too	High due to direct verification	Low, resource-heavy due to the need for a large staff, limits scalability
SMS based consent	High, relatively private, and avoid excessive data collection	Very high, quick and simple	Low since it risks circumvention in case of children accessing OTP	Very high scalability with robust SMS infrastructure
Zero Knowledge Proof	High, preserving privacy through cryptographic proofs	High, easy to use	High precision depends on verifier and algorithm integrity	Moderate, requires advanced infrastructure and resources
Operating System/ App store	Moderate, relatively private, integrates with parental controls	Moderate, dependent on parents' understanding of digital platforms	Moderate depends on parental literacy and diligence	Highly scalable due to integration into existing ecosystems
Interoperable VPC	High, because of avoidance of repeated identity verification	High, easy to implement as parents' identity has already been established	High because one platform has already done the due diligence	High, as platforms can access already established identity through interoperable mechanisms

A market-driven approach—where platforms choose and transparently disclose their verification methods—would encourage competition, fostering more effective, user-friendly solutions. This flexibility would be particularly beneficial for smaller platforms, allowing them to adopt cost-effective yet secure verification processes, while larger platforms could implement more comprehensive systems based on their resources.

We recommend that the DPDP Rules should avoid rigid, one-size-fits-all approaches to VPC to encourage innovation and experimentation. A non-prescriptive, risk-based approach should be adopted, allowing service providers to choose verification methods based on use case, risk level, and implementation capabilities. Lower-risk activities like viewing general content can rely on simple self-declaration, whereas high-risk activities such as accessing age-restricted content or financial transactions require robust verification.

Additionally, an interoperable VPC framework should be incorporated, similar to interoperability in telecom and payments, enabling platforms to share verified consent securely. This would reduce data collection, ease compliance burdens, and enhance efficiency, particularly for smaller platforms. For instance, if a parent is already verified on one platform, their verified identity should be usable by another platform, minimising the need for repeated verification and improving digital accessibility.

To balance innovation and child protection, an independent advisory group of consumer organisations, technical experts, and child development specialists should be established. This group would develop standards, manage grievances, assist small businesses, and promote responsible data handling by suggesting minimal data collection, restricted biometric processing, and user anonymity. Over time, it would assess VPC implementation, identify risks, propose mitigations, and educate policymakers, service providers, and parents to ensure safety, privacy, and accessibility remain central to the system's evolution.

Read the full report here.

This Snapshot of Findings is prepared by Asheef Iqubbal and Krishaank Jugiani, Senior Research Associates, CUTS International as a part of the project titled 'Economic Analysis of Verifiable Parental Consent Mechanisms', along with guidance, support and inputs from Amol Kulkarni, Director Research, CUTS International.

CUTS International, D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India. Ph: +91.141.228 2821, Fx: +91.141.228 2485,
E-mail: cuts1@cuts.org, Web: www.cuts-international.org.

Also at Delhi, Calcutta and Chittorgarh (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); Geneva (Switzerland); and Washington DC (USA).

March, 2025