ECONOMIC ANALYSIS OF VERIFIABLE PARENTAL CONSENT MECHANISMS

Evaluating Impact on Consumers and Data Fiduciaries

CUTS International
1983-2023

#2505

Economic Analysis of Verifiable Parental Consent Mechanisms

Evaluating Impact on Consumers and Data Fiduciaries

Economic Analysis of Verifiable Parental Consent Mechanisms

Evaluating Impact on Consumers and Data Fiduciaries

Published by

CUTS International
D-217, Bhaskar Marg, Bani Park, Jaipur 302016, India
Tel: +91.141.2282821, Fax: +91.141.2282485
Email: cuts1@cuts.org, Web site: www.cuts-international.org

Authors:
Asheef Iqubbal, Senior Research Associate, CUTS International
Krishaank Jugiani, Senior Research Associate, CUTS International

Citation: Iqubbal, A. & Jugiani, K. (2025). *Economic Analysis of Verifiable Parental Consent Mechanisms: Evaluating Impact on Consumers and Data Fiduciaries*. CUTS International.

Cover Image Credit: *LiveMint*

© CUTS International, February 2025

The material in this publication may be reproduced in whole or in part and in any form for educational or nonprofit purposes without special permission from the copyright holders, provided the source is acknowledged. The publishers would appreciate receiving a copy of any publication which uses this publication as a source.

Content

Foreword **4**

Acknowledgements **5**

Executive Summary **6**

1. Introduction **11**
Methodology and Approach 13

2. The Draft Digital Personal Data Protection Rules, 2025 ..... **19**

3. Age Assurance and Parental Consent: Mechanisms, Challenges and Associated Costs **23**
Methods for Age Assurance and Obtaining VPC 25

4. Conclusion and Recommendations **46**
Conclusion 46
Recommendations 48

Dr. Sasmit Patra
MEMBER OF PARLIAMENT
RAJYA SABHA

Foreword

22nd March, 2025

Economic Analysis of Verifiable Parental Consent

This study by CUTS International presents a timely and in-depth analysis of the economic and operational challenges of implementing VPC mechanisms in the Indian context. Through a comprehensive mixed-methods approach, the study triangulates publicly available cost data from global service providers, in-depth literature reviews, and stakeholder consultations. Importantly, it evaluates not only the monetary costs, but also the indirect trade-offs such as privacy concerns, scalability, and accuracy of various methods.

The report notes that prescribed methods in the draft Rules may be neither cost-effective nor privacy-preserving, with estimated annual costs of US$101,440 for government ID-based verification and US$45,436 for DigiLocker-based verification. While these methods offer accuracy, they raise concerns around privacy, exclusion, and the burden of storing sensitive data. These measures may disproportionately affect children, marginalised groups, and smaller platforms, potentially restricting access to essential digital spaces and stifling innovation. The report rightly recommends a non-prescriptive, risk-based approach that allows platforms to adopt context-appropriate verification methods, alongside interoperable consent frameworks for platforms to share verified consents securely, and guidance from an independent multi-stakeholder body, helping to balance user protection with inclusivity, cost-efficiency, and innovation.

The CUTS team must be appreciated for this meticulously researched contribution to the discourse. I hope this study will inform ongoing regulatory deliberations and foster constructive dialogue among policymakers, industry leaders, and civil society, on how children can be effectively protected through a flexible, context-sensitive approach that balances safety with accessibility.

Dr. Sasmit Patra

C-104, Swarn Jayanti Sadan, Dr. B. D. Marg, New Delhi-110001, INDIA
Tel.: +91-11-23314809 | Email: sasmit.patra@sansad.nic.in

Acknowledgements

The report is the culmination of collaborative efforts from numerous individuals who contributed their insights, expertise, and support. We extend our gratitude to Amol Kulkarni, Director (Research) at CUTS International, for his constant guidance, thought-provoking discussions, and leadership throughout this project.

Our sincere thanks to Dr. Sasmit Patra, Member of Parliament, Rajya Sabha, and Member, Parliamentary Standing Committee on Communications and Information Technology, for kindly writing the foreword and lending valuable support to this initiative.

We are particularly indebted to the digital startups, civil society organisations, law firms, and academics who generously shared their time and valuable perspectives, enriching our understanding of the landscape. Special mention goes to verifiable parental consent service providers, whose expert inputs shaped our research findings.

The report benefited from the dedicated support of our colleagues: Samridh Shastry, Aakarsh Bhargav, Pratyush Banerjee and Sobhan Guha. We are also grateful to Nishchay Rao (Intern at CUTS International) for his valuable contributions to this report.

The Publications Team at CUTS International-Madhuri Vasnani, Rajkumar Trivedi, and Mukesh Tyagi-deserve special recognition for their exceptional effort in bringing this report to fruition.

We acknowledge the contributions of other individuals who, while not named here, played crucial roles in this project's success.

Any errors or omissions that remain are solely our responsibility.

Asheef Iqubbal and Krishaank Jugiani
Senior Research Associates

Executive Summary

The Digital Personal Data Protection (DPDP) Act, 2023, mandates Verifiable Parental Consent (VPC) under Section 9. As children are increasingly engaged with digital services like education and entertainment, ensuring their safety is a legitimate need. The government released the Draft Digital Personal Data Protection Rules, 2025 (Draft Rules) for public consultation. The draft Rules seek to implement the Act's provisions by requiring parents or guardians to verify their identity and provide consent before an individual under 18 can register on an online platform.

The Rules propose two methods for verifiable parental consent on digital platforms. For parents who already use the platform, platforms can verify their age and identity using previously provided information. If the parent does not use the same platform, verification can be done through a legally authorised entity or government body. The draft Rules propose that digital platforms exercise "due diligence, for checking that the individual identifying herself as the parent is an adult who is identifiable if required in connection with compliance with any law."

The mandated approaches – either using existing platform data or government-authorised digital services – can impose substantial burdens, particularly on smaller platforms with limited resources. This may include costs related to complying with mandated technical requirements, such as integrating with government-authorised entities or referencing reliable identity and age details available with the platform or entity. It could also lead to friction among minors and parents, negatively impacting engagement, consumer satisfaction, and revenue streams across platforms. This binary approach in the draft Rules overlooks several VPC methods and diverges from global approaches, which provide greater flexibility.

As underscored in our report, the proposed methods are neither the most cost-effective nor entirely secure and accessible. Better alternatives exist and should be considered under the draft Rules.

Further, the draft Rules fail to consider the varying risk levels across different digital platforms and instead mandate a one-size-fits-all approach that may not be

appropriate for all platforms. Regardless of the risks involved, all data fiduciaries are required to ensure the parent's identity and age can be verified, often requiring a combination of documents already held by the fiduciary or identity data from government-authorised services. This makes compliance both challenging and costly.

Additionally, not all parents and children will use the same platform. In such cases, the draft Rules suggest only one method of verification, which is dependent on DigiLocker. This limits flexibility, as platforms may not be allowed to explore innovative and experimental approaches to meet compliance requirements. Encouraging innovation, interoperability and competition in this space could reduce costs and increase efficiency, especially for smaller platforms that may lack large databases for referencing and obtaining verifiable parental consent.

Moreover, one interpretation of the draft Rules indicates that platforms might be held responsible for verifying users' ages, which would effectively require verification of all users of digital services. This proposed age verification requirement creates a fundamental shift away from anonymous internet access.

Further, these processes are often time-consuming, cumbersome, and costly, which may involve integrating an additional step for age assurance. These costs will be due to operational steps like recurring subscription fees for the software, staff training, etc., collecting information, such as behavioural data, government-issued IDs, financial details, storage costs, and ongoing verification processes. This can lead to financial strain, disproportionately impacting smaller platforms and startups. Initial estimates in other countries like the U.S. suggest that the costs of verification could range from US$35,000 in developing infrastructure to US$70,000-120,000 in ongoing annual costs.[1]

The implementation of VPC systems may also impact a range of digital services, particularly considering that 29.9 percent of internet users are between ages 0 and 17.[2] These young users engage with online platforms for diverse purposes, with many services specifically designed for them.[3]

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/

India's startup ecosystem, ranked third globally with over 31,000 startups, may face particular challenges from these requirements. The ecosystem is nearly evenly split between business-to-consumer (B2C) (51 percent) and business-to-business (B2B) (49 percent) services.[4]

These startups, particularly B2C, may have to identify, estimate, or verify user ages and secure verifiable parental consent where necessary. The financial impact of these requirements would fall disproportionately on startups, who must absorb both direct implementation costs and indirect effects on user acquisition and retention.[5]

Further, VPC mechanisms pose critical privacy and security risks, especially those which may involve intrusive data collection and storage. Verification systems requiring sensitive personal data, such as biometric identifiers, age, government-issued IDs, or financial details, create data breaches and misuse vulnerabilities. Startups and smaller platforms, often lacking robust cybersecurity infrastructure, are particularly at risk. A data breach involving parental consent data could result in severe financial losses, reputational damage, and legal liabilities.

Further, intrusive verification methods, like facial recognition or video identification, raise concerns about profiling, data retention, and user tracking, undermining privacy protection. Additionally, VPC systems may deter children from accessing platforms, limiting opportunities for learning, social interaction, and skill development, putting Indian youth at a disadvantage in an increasingly digital economy.

While more efforts are required to ensure that children can safely access online spaces, current technical and consequent financial requirements often mean that VPC mandates may introduce compounding risks and barriers. Many social media platforms already implement age assurance methods to comply with existing regulations and uphold their own global terms and conditions. For example, Instagram asks users to submit their date of birth upon signup to confirm they are 13+.[6]

---

4 https://itic.iith.ac.in/downloads/NASSCOM%20Zinnov%20Indian%20Tech%20Startup%20Report%202024.pdf

5 Several platforms serving young users may require repeated parental consent, especially if services are used intermittently. This could mean children need parental approval each time they access the platform, disrupting the seamless experience young users expect. Frequent requests deter engagement, prompting platforms to invest resources in maintaining user interest and potentially increasing costs passed on to consumers. This creates challenges for both users and providers, complicating the digital experience and undermining its convenience.

6 https://help.instagram.com/2387676754836493

Although these methods are not without flaws. Given the implications of VPC and the potential for unintended consequences, users, lawmakers, regulators, industry stakeholders, and civil society must comprehend the complexities and challenges inherent at each stage. This report assesses the different risks and costs around VPC and the necessity of a balanced, risk-based, and proportionate framework for VPC to minimise unintended consequences while maximising safety, security, privacy, and accessibility for users.

Key Recommendations

- Regulatory frameworks should avoid prescribing rigid, one-size-fits-all solutions to meet the requirements of the VPC, which may harm innovation and experimentation. We recommend a non-prescriptive, risk-based approach to VPC, focusing on context-appropriate solutions by encouraging different models to be experimented with.

  The Rules should consider allowing service providers to choose verification methods based on their use case, risk level, and implementation capabilities, recognising that different scenarios require varying levels of scrutiny. Lower-risk activities, such as viewing general content and writing product reviews, can use simple self-declaration methods. In contrast, high-risk activities like age-restricted content or financial transactions require more robust verification.

- We recommend that the Rules incorporate an interoperable, verifiable parental consent framework. Similar to interoperability in sectors like telecom and payments, platforms should be allowed to establish secure protocols for sharing verified consent. This would minimise data collection, ease compliance burdens and improve efficiency, particularly for smaller platforms. Standardised protocols should enable secure communication while ensuring data protection.

  Suppose a parent has already been verified on one platform, and their child wishes to use another platform where the parent is not registered. In that case, the minor should be able to direct the new platform to retrieve the verified identity from the platform the parent is using. This would enable seamless communication between platforms, simplifying verification. Parents would only need to verify once, reducing barriers to digital participation, especially in regions with limited access to government ID services, digital infrastructure, or digital literacy.

- We recommend establishing an independent group of consumer organisations, technical experts, and child development specialists to balance innovation and protection. The group can develop codes and standards, suggest mechanisms to pool resources for small businesses, manage grievances, and resolve disputes. It would establish baseline requirements for responsible data handling, including minimal data collection, restricted biometric processing, and user anonymity.

  After a specified period of time, the group would review VPC implementation, assess effectiveness, identify risks, and explore mitigating strategies and alternate solutions. Beyond assessment, the group would educate policymakers, service providers, startups, and parents on VPC methods, risks, and alternatives. Continued engagement with relevant stakeholders would ensure safety, privacy, and accessibility remain central to system design.

1 Introduction

The Digital Personal Data Protection (DPDP) Act, 2023[7] received Presidential assent on August 11, 2023. The Act focuses on individual consent, giving users greater control over their data.[8] It offers an additional layer of protection for children under the age of 18 and individuals with disabilities. Section 9, in particular, deals with the governance of children's data.

The recently released draft of DPDP Rules proposes that data fiduciaries must verify that individuals claiming to be parents are identifiable if required in connection with compliance with any law for the time being in force in India. The draft Rules prescribe two verification methods: using existing platform data for current users or verifying through government-authorised entities or virtual non-user tokens. This binary verification approach contrasts with global standards that provide greater flexibility in obtaining verifiable parental consent.

The implementation of VPC requirements would significantly impact digital access patterns among India's adolescent population. A recent study indicates widespread smartphone accessibility among 14-16-year-olds, with approximately 90 percentreporting smartphone presence in their households. While device access is near-universal, personal ownership follows an age-gradient pattern–increasing from 27 percent among 14-year-olds to 37.8 percent among 16-year-olds.[9]

Digital literacy metrics reveal that over 80 percent of this age group possesses basic smartphone operation skills, though a notable gender gap exists. Social media users are aware of basic online safety measures – 62 percent understand profile blocking/reporting mechanisms, 55.2 percent know privacy settings management, and 57.7 percent can execute password changes. However, these safety awareness levels

7 Hereinafter referred to as "the Act" or "DPDP Act".

8 The Digital Personal Data Protection Act, 2023, available at: https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

9 https://asercentre.org/wp-content/uploads/2022/12/ASER_2024_Final-Report_25_1_24.pdf

are consistent with gender disparity, with boys showing higher familiarity across most states.[10]

A CUTS study also shows that over 75 percent of parents believe their child knows more about online safety practices and can consent to service terms, a view supported by 73 percent of young users.[11]

However, awareness often does not translate into practice, making ensuring minors' safety in the digital space essential.[12] In a digital economy where young users are increasingly using services for online shopping, entertainment, and other areas, offering age-appropriate protection is both practical and necessary. This has led to efforts such as age-gating, filtering adult content, and providing security and protective services to children.[13] The aim is to mitigate risks to children on digital platforms, such as exploitation, grooming, harassment, stalking, and profiling.

Consent is the foundation of lawful data processing, which ensures individuals have control over how their personal information is used. However, when users are unable to provide consent or enter into a contract, such as minors or individuals with limited legal capacity, the responsibility typically falls to a parent or legal guardian. This intends to ensure that decisions about data processing are made by someone who can act in the best interests of the minors, upholding their rights and protecting their privacy.

Policymakers are rightfully concerned about protecting young internet users, but mandating VPC comes with trade-offs. Major jurisdictions such as the European Union, the UK, the U.S., and Australia are experimenting with regulations, yet debates on these approaches remain open. Concerns persist about the complexity and cost of implementing VPC methods. Some of the methods include credit card verification and government ID authentication, OTP validation or signed consent forms.

Each method comes with risks, costs, benefits, and challenges such as privacy, convenience and scalability. The costs involved can be both direct and indirect. Direct

[10] https://asercentre.org/wp-content/uploads/2022/12/ASER_2024_Final-Report_25_1_24.pdf

[11] https://cuts-ccier.org/pdf/slide-deck-protecting-childrens-data-analysing-perspectives-of-parents-children.pdf

[12] https://cuts-ccier.org/pdf/slide-deck-protecting-childrens-data-analysing-perspectives-of-parents-children.pdf

[13] See Section 9, DPDP Act

costs refer to the monetary expenses required to establish the necessary technological infrastructure and daily operations. Indirect costs, on the other hand, include the efforts needed to ensure the effectiveness and scalability of the mechanism while maintaining privacy.

This report proposes frameworks for policymakers and platforms to allow space for innovation while prioritising child safety and data protection. While policymakers' intentions are legitimate, factors such as parental digital literacy, security, privacy, and the monetary costs of establishing VPC mechanisms must be carefully considered when assessing solutions for its implementation. Thus, VPC requirements should align with risk levels, allowing service providers to choose suitable methods based on their context. The focus should be on achieving protective outcomes through flexible, context-driven approaches.

Service providers should implement VPC that balances user protection with accessibility and privacy. This involves selecting verification methods suited to the service's risk level, user base, and technical capabilities. Platforms should minimise data collection, implement necessary steps like anonymisation, and regularly assess the effectiveness of their systems, adjusting as needed.

Methodology and Approach

We have assessed the costs mentioned above using a combination of publicly available data from service providers and our own requirements, which include engaging with minors for surveys and capacity-building initiatives. We triangulated these datasets with an in-depth literature review to develop a well-rounded cost estimate, drawing on academic papers, policy briefs, expert opinion pieces, and case studies. This allowed us to cross-reference data from multiple sources and perspectives, ensuring a clear, indicative understanding of the potential costs involved in the Indian context.

Further, we conducted stakeholder consultations with a range of experts, including academics, service providers, VPC solution providers, legal researchers, and child rights advocates, to gather their insights on the accessibility, costs, privacy concerns, and scalability of different VPC methods.

While the final cost estimates are indicative, as these services have not yet been fully implemented in India, our analysis is based primarily on providers' costs in the UK, U.S., and Europe. These regions already have laws mandating VPC without prescribing

specific technological tools. Although these providers operate within different regulatory contexts, they are hopeful to make their products compliant with India's DPDP Act. They have indicated that the costs would likely be similar to those in their respective regions, with the primary variation depending on the scale of the operation.

The report is structured around essential constructs of the VPC: age assurance, parental consent processes, and associated costs, which include indirect costs, such as privacy concerns, accuracy, and the effectiveness of these mechanisms. Section 2 discusses the approaches prescribed in the draft Rules and provides an analysis of these approaches.

Section 3 explores the various mechanisms involved in age assurance and obtaining verifiable parental consent for users under 18. It examines various age assurance and parental consent mechanisms, evaluating their strengths, limitations, and effectiveness. It also addresses the monetary costs of implementing each method, including the infrastructure needed for age assurance, consent collection, and data storage.

Section 4 concludes with recommendations and an optimal way forward. A summarised matrix of the costs and features of different methods has been provided upfront.

Matrix of Different Methods

Based on the discussion in the report, a comparison matrix of different methods in terms of cost, privacy, convenience, accuracy, and scalability is provided:

Estimated Costs (for 1,000,000 annual verifications)[14]

Method	Infrastruc-ture/Setup Cost (A)	Opera-tional Costs (B)	Storage Costs (C)[15]	Total Cost (A +B +C)	Total Cost (Average)	Cost Scale (Low To High)[16]
Self Declaration	10,000	818 – 996	260	11,078 – 11,256	11,167	Low
Age Estimation (AI/ML)	7,800	494,618[17]	260	502,678	502,678	High
Governmen t-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[18]	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[19]	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/	25[20]	1,764 – 3,727[21]	260	2049 – 4012	3,031	Low

[14] All the costs are in US$ and rounded off

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

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

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

[18] 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.

[19] The average storage costs for the video file discussed above have been taken.

[20] for Google Play Store.

[21] Includes US$99 annual fee for Apple.

Method	Infrastruc-ture/Setup Cost (A)	Opera-tional Costs (B)	Storage Costs (C)[15]	Total Cost (A +B +C)	Total Cost (Average)	Cost Scale (Low To High)[16]
App store						
Interoperable VPC	10,000	Shared between platforms	260	10,260	10,260	Low

Features

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 and 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
KBA	Moderate to high privacy risks if knowledge about personal data is assessed	Moderate and avoids the need for additional hardware, but users may face frustration due to a	Moderate since it is vulnerable to generic or inaccurate answers	Low, costly and challenging to scale

Method	Privacy	Convenience	Accuracy	Scalability
		set of personal questions		
Third-Party Verification	Low privacy and 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; however, it assumes that most people will have email IDs
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 having access to OTP	Very high scalability with robust SMS infrastructure
ZKP	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

The analysis of various verifiable parental consent methods shows that the government's prescribed approaches in the DPDP draft Rules for age and identity verification — whether through existing platform data or authorised government entities such as Digital Locker services — may not be the most optimal in terms of security, cost, and efficiency.

Alternative methods could offer better solutions while maintaining the minor's and parents' security. Rather than mandating specific verification channels, the draft Rules would benefit from allowing platforms to implement solutions that best suit their technical capabilities and user needs.

A market-driven approach, where platforms can choose and transparently disclose their verification methods, would help parents make informed decisions about which platforms best protect their children while respecting their preferences. This competitiveness in the ecosystem would drive innovation, leading to more efficient and user-friendly solutions.

Such flexibility would be especially valuable for smaller platforms, allowing them to choose cost-effective solutions without compromising the security of their users. In comparison, larger platforms could opt for more comprehensive systems based on their resources and user base.

2 The Draft Digital Personal Data Protection Rules, 2025

On January 03, 2025, MeitY released the Draft Digital Personal Data Protection Rules, 2025 ("draft Rules" or "the Rules") for public consultation. Rule 10 specifies the obligations of data fiduciaries to obtain verifiable parental consent before processing children's personal data. The rule requires data fiduciaries to verify the age and identity of individuals claiming to be parents before obtaining verifiable parental consent to process the data of users under 18. Platforms can choose how to verify this through existing user information or government-authorised virtual tokens–digital locker services.

As per the draft Rules, platforms would have to implement technical and organisational measures to ensure consent is obtained before processing begins, and due diligence must be conducted to confirm the parent is an identifiable adult.

The Rules prescribe two methods for parental verification:

- ***Existing Platform User:*** If the parent is already a user of the **same** platform, their previously provided age and identity information can be used. For example, Instagram can verify a parent's status using their existing account details when their child requests an account.
- ***Non-Platform User:*** If the parent is not a user of the same platform, platforms can verify their age and identity through a legally authorised entity, a government body, or a virtual token system. This token links to the parent's voluntarily provided identity and age details, stored with a digital locker service provider. For instance, if parents are not on Snapchat, Snapchat can verify a parent's information through these authorised channels.

When a minor attempts to create an account on digital platforms, two scenarios could unfold in the wake of the draft Rules: In the first scenario, where the parent already uses the platform, the process would begin with the teen entering their age during signup. The platform would then pause the registration and request the parent's username.

Following this, the parent would receive a comprehensive notification detailing their child's requested permissions, the types of data to be collected, and its intended uses. Using their verified account, the parent can then review these permissions and make a decision to either approve or deny the request.

Suppose parents are not users of the platform their child is trying to access. In that case, verification can be completed using a virtual token from a Digital Locker service provider or by submitting a government-issued ID through an authorised government mechanism. The platform will then verify the parent's identity and age before allowing the child to create an account.

While the draft Rules propose much-needed clarity on the operationalisation of VPC, they raise critical questions about implementing these requirements. A key challenge is how platforms will reliably determine users' ages. The proposed Rules may require platforms to ensure that a child's data is not processed without verifiable parental consent. Even if a user declares themselves an adult, platforms may need to monitor user behaviour to verify whether they are actually an adult or a child. This assumption is reinforced by the requirement for platforms to exercise due diligence and ensure that information likely to harm children is not accessible to them.

Moreover, the Rules also indicate how to verify an adult's age and identity. However, they lack protocols to confirm whether that adult is the child's parent or legal guardian. This gap creates potential misuse, where adults could falsely claim parental status to develop children's accounts.

Further, the Rules also appear to suggest excessive data collection. For instance, why the parent's or legal guardian's age is required is unclear. Indian law establishes 18 as the minimum age for parenthood through various legal frameworks, including marriage laws. While Rules propose methods for obtaining verifiable parental consent — including using existing user data or government-authorised digital tokens — they may not always be the most optimal solution, and other options should be considered. It may create barriers in terms of compliance, innovation, and consumer choice.

Users who are unwilling or unable to store identity and age documents in DigiLocker may be unable to verify their status as legal guardians. This could hinder platform adoption and engagement, especially among individuals with limited digital access or concerns about the privacy of centralised data storage.

Furthermore, even in sectors like education and skilling, online gaming, entertainment, etc., children commonly use platforms that their parents might not use. This means parents may not have accounts with the same platforms their children may be using. Even if parents and children engage in similar sectors, like entertainment and social media, they may not have accounts on the same platforms, complicating the VPC process. Inter-platform communication for verification purposes may not be allowed, meaning each service must conduct independent verification through prescribed channels.

In contrast, global practices often permit third-party verification services to facilitate such processes. Requiring VPC in such cases would necessitate mechanisms involving parents who are not part of the platform's user base, increasing the technical and administrative burden on service providers. This would disproportionately affect smaller platforms, which may struggle with technical integration and the practical challenge of having both parents and children as users, raising concerns about distorted competition in the ecosystem.[22]

The financial burden of compliance and efficiency issues related to the proposed mechanisms for obtaining VPC will likely result in higher service fees for consumers or reduced access to affordable digital services.

Moreover, the Rules fail to account for varying risk levels across different digital platforms, so they apply a one-size-fits-all approach that may be overly restrictive. Online services pose distinctly different risks to minors as they carry varying levels of risk based on functionality and design.

Some, like those enabling anonymous interactions, pose clear risks such as grooming or extortion. Others, with sticky features, make it hard for children to disengage from their devices. In contrast, some services may offer positive age-specific features, such as 'time-outs' or easy disengagement. For example, a service that follows data minimisation, has no direct messaging and excludes adult material may carry lower risk.

However, as per the draft Rules, all the data fiduciaries may have to ensure the parent's identity and age are verifiable, which may involve multiple document combinations

[22] https://www.financialexpress.com/life/technology-parental-consent-smaller-platforms-say-they-face-disadvantage-against-big-technbsp-3715261/?utm_source=chatgpt.com

already held by the fiduciary or identity data from government-authorised services, making compliance challenging and costly. As referenced, verifications through government-issued IDs cost around US$101,440 annually, while for DigiLocker, it may cost around US$45,436 annually. Platform compliance costs could be passed on to consumers, resulting in higher costs for them.

Finally, the Rules raise concerns about broad-based age verification requirements, which could further complicate platform operations and user accessibility. As VPC is an evolving area globally, with various methods available to meet its requirements, Indian regulation should encourage innovation and experimentation. This approach would help address the country's diverse realities while ensuring a balance between safety, convenience, privacy, and accessibility.

Moreover, a more nuanced, risk-based approach would better serve both platforms and users by adjusting compliance requirements based on platform risk levels, encouraging innovation and competition in verification methods among compliance solution providers. The rule should allow platforms to be interoperable in the ecosystem, eliminating the need for each platform to build costly in-house verification systems.

For example, while building an in-house product could cost around US$25,000-50,000.[23] Third-party verifiers charge an annual fee of less than US$300.[24] This would be especially valuable when parents and children use different platforms. It would make compliance more feasible for smaller operators while maintaining appropriate safety standards based on actual risk levels.

[23] https://engineadvocacyfoundation.medium.com/more-than-just-a-number-costs-and-business-impacts-on-startups-of-determining-user-age-ceabe03d40b1

[24] Third-party method of verification, page 22.

3 Age Assurance and Parental Consent: Mechanisms, Challenges, and Associated Costs

U.S. Children's Online Privacy Protection Act (COPPA), one of the first laws in this area, set a precedent by allowing platforms to ask users their age. Under COPPA, platforms must obtain verifiable parental consent only if a user reports being under 13. While this simplifies registration, it is prone to age misrepresentation. To address this, regulators have been exploring guidelines on age assurance.

Though not universally defined, "age assurance" broadly refers to methods platforms use to verify age and enforce age restrictions along with age-specific content and data processing provisions. Although COPPA does not mandate any specific method of obtaining parental consent, the Federal Trade Commission, the body overseeing the compliance of COPPA, has outlined several consent methods that meet its standard in light of available technology. These include:[25]

- having parents sign and return consent forms via fax, mail, or electronic scan;
- using payment systems that notify account holders of transactions;
- calling a toll-free number or connecting via video conference with trained personnel;
- providing and verifying government-issued IDs (with the ID deleted post-verification);
- requiring parents to answer knowledge-based challenge questions or
- submitting a photo ID verified through facial recognition technology

From an operational perspective of the DPDP Rules, the requirement of obtaining VPC may involve:[26,27]

- Determine the age of the user
- Reach out to parents and/ or legal guardians for the consent
- Validate the legitimacy of the relationship between the parent/guardian and the child.

[25] Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business | Federal Trade Commission

[26] THE STATE OF PLAY: - Is Verifiable Parental Consent Fit For Purpose?

[27] How should we obtain, record and manage consent? | ICO

- Validate the identity and age of the parent/ legal guardian providing consent.
- Obtain verifiable consent from the parent or legal guardian.

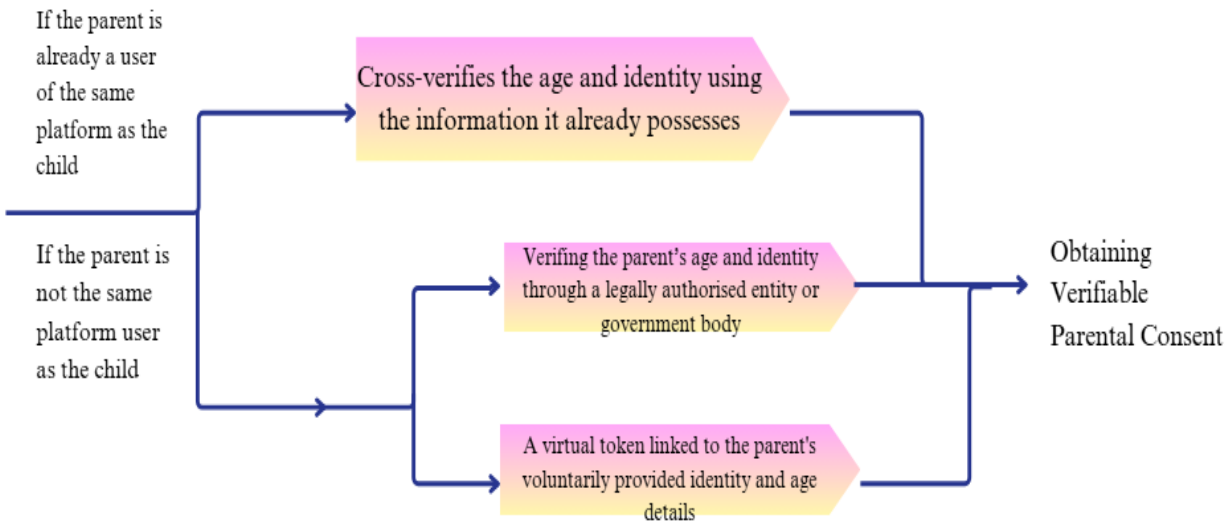
The draft Rules outline a framework for obtaining parental consent. The parent or legal guardian will verify a child's age using a government-mandated ID or a token issued by a Digital Locker service provider. The Rules also propose scenarios where parents are already users of the platform as well as situations where they are not.

While using existing data held by service providers to verify parents' identity and age allows children to avoid repeated verification, its implementation may raise concerns. The reliability of this verification method remains uncertain and may raise concerns about distorted competition. Larger platforms with a more extensive user base could have greater control over authentication systems, potentially reinforcing their dominance in the market.[28]

While currently, the Rules limit obtaining VPC through available data from fiduciaries and government-authorised entities, they do not account for the wide range of mechanisms available for obtaining VPC. Globally, many platforms have been allowed to integrate third-party verification services or even consent management platforms to ensure secure, verifiable parental consent without relying solely on government systems and/ or existing data available with data fiduciaries.

These alternative methods can offer more flexible, cost-effective, privacy-preserving, scalable, and user-friendly solutions, particularly for smaller platforms or those operating in regions with uneven digital infrastructure. Thus, there is room for further specification regarding the methods to be employed and associated costs, as discussed below.

[28] https://5rightsfoundation.com/wp-content/uploads/2024/09/But_How_Do_They_Know_It_is_a_Child-1.pdf



Methods for Age Assurance and Obtaining VPC

Various mechanisms are being considered for age assurance and obtaining verifiable parental consent. These include methods such as self-reporting, AI-based age estimation, using a credit or debit card, video conferencing, and government or ID submission.[29] However, each approach has its own advantages and challenges related to privacy, security, convenience, accuracy, cost and scalability.

Setting up and Integration Costs

The cost of software for each VPC method varies depending on its features, functionality, and the level of security it provides. Basic age assurance solutions are typically available for a one-time fee of approximately US$200. However, more advanced systems that incorporate features such as facial recognition or biometric authentication can cost up to US$5,000.

For organisations requiring multiple user access points and enhanced security measures, the expenditure can rise significantly, ranging from tens of thousands to several hundred thousand dollars, depending on the complexity and scale of implementation.[30] This could disproportionately impact startups and small businesses, which run on limited resources and focus on product development for their users.

[29] https://5rightsfoundation.com/wp-content/uploads/2024/09/But_How_Do_They_Know_It_is_a_Child-1.pdf

[30] https://slashdot.org/software/age-verification/

However, these costs extend beyond initial purchase or licensing fees and often include expenses for custom development, integration, and ongoing subscriptions. API (Application Programming Interface) acts as a bridge that enables different software systems to communicate with each other. The backend is the server-side infrastructure that handles data processing, storage, and application logic.

For a VPC system, API development will involve designing specific protocols that allow websites or apps to connect with a parental consent service. This can either be a third-party VPC service provider or a service provider's own VPC service.[31]

Initial API integrations can cost US$1,000 to US$5,000, depending on the complexity of the integration and the platforms involved.[32] An age assurance solution provider confirmed that the system integration cost may be around US$10,000 (INR ₹8,50,000 approx., based on a conversion rate of US$1 = ₹85).

For the sake of simplicity and convenience, this report assumes an integration/API cost of US$10,000 across all methods unless otherwise specified. It is important to note that actual costs may vary based on factors such as company size, the specificity of the chosen method, and the complexity of implementation.

Operational Costs

The costs discussed below are ongoing expenses required to manage and maintain the VPC system, such as verification, storage, service subscriptions, etc.

Most age assurance services operate on a subscription-based pricing model, with monthly fees typically ranging from US$50 to US$500. Low-cost solutions usually range between US$50 and US$100 per month and offer basic features such as document verification and database checks. These systems are cost-effective but may lack advanced capabilities like biometric verification. They are well-suited for businesses dealing with low-risk products and seeking affordable compliance options.[33]

---

31 For example, when a child tries to register for a service, the API sends a request to the parental consent system, triggering actions such as sending notifications to parents for verifiable parental consent. Backend integration ensures that these API interactions are securely managed and that data flows seamlessly between the parental consent system service provider and any external verification services (e.g., identity authentication providers).

32 https://amasty.com/blog/age-verification-compliance/

33 Ibid

On the other hand, premium solutions typically start at US$300 per month and can scale significantly based on features and usage. These systems often include advanced verification technologies, such as AI-driven age estimation and multi-layered ID checks. They are primarily designed for high-risk industries, including alcohol sales, where strict regulatory compliance and robust verification processes are essential.[34]

In addition to verification services, storing consent documents also incurs costs. For example, to store 10,00,000 consent documents in pdf format (est. 1 MB each),[35] approximately 976.56 GB of storage is required. Cloud storage costs vary by provider, ranging from ₹1.52[36] to ₹1.9[37] per GB per month. This results in a monthly expense of ₹1,484.37 to ₹1,855.46 (US$17.81 to US$22.26) or an annual total of ₹17,812.44 to ₹22,265.52 (US$213.75 to US$267.19). For consent through video file (est 100 MB each),[38] the total storage requirement is approximately 97,656 GB. This amounts to monthly storage costs of ₹148,470.12 to ₹185,456.40 (US$1,767.50 to 2,207.81) and annual storage costs of around ₹1,781,641.44 to ₹2,225,476.80 (US$21,209.06 to 26,494.29).

Cost Implications of Different Age Assurance and VPC Methods

These methods for age assurance and obtaining VPC vary in their approach and implementation, leading to differences in cost implications, privacy, security and convenience concerns that need to be carefully assessed. The costs associated with VPC methods depend on factors such as the additional technical infrastructure (implementation costs) required for some specific process and the necessary operationality and scalability for each mechanism.

Further, additional costs may arise at various stages of the VPC methods, such as verifying consent, securely processing data, and responsibly managing information through storage or deletion protocols. Hence, analysing these costs is crucial for platforms to achieve a balance between compliance, user experience, and operational efficiency, as well as for consumers, who may bear these costs directly or indirectly.

The image given below illustrates the different methods for age assurance.[39]

---

34 Ibid

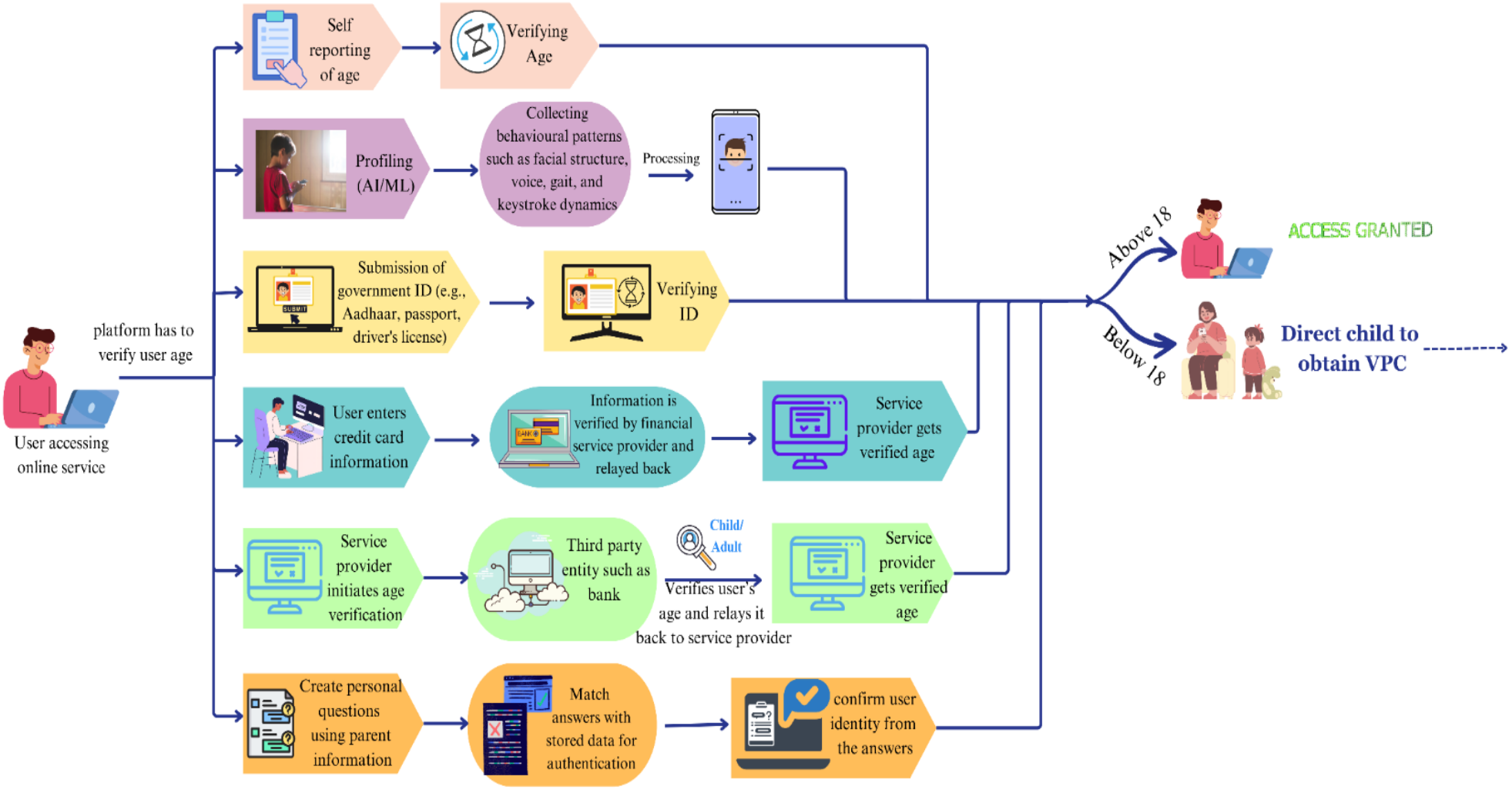
35 Consent Letter For GST Registration: Format and Requirements.

36 https://azure.microsoft.com/en-gb/pricing/

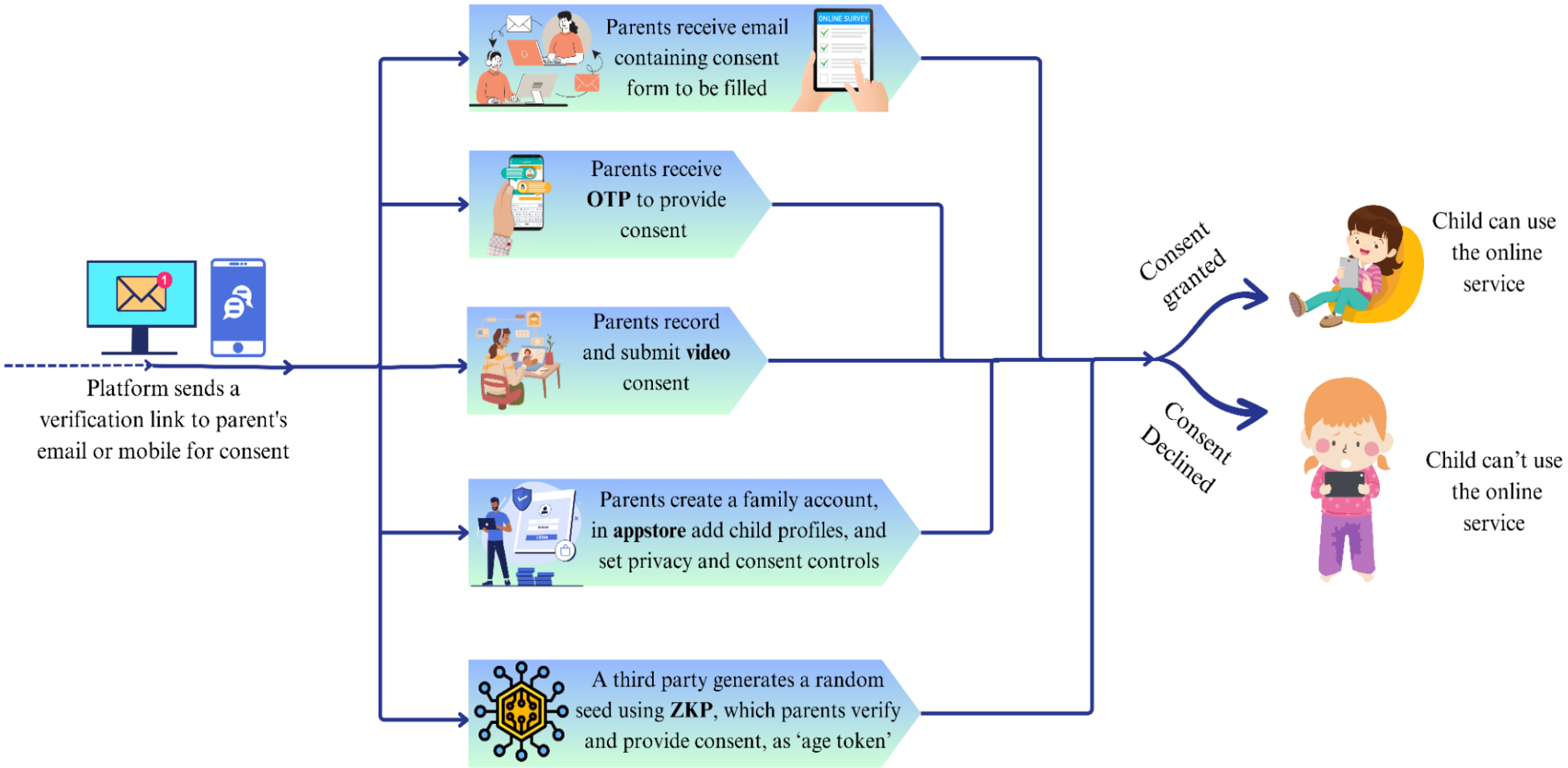
37 https://aws.amazon.com/pricing/

38 https://elearning.uq.edu.au/guides/video-and-audio-upload/video-file-size-recommendations

39 Authors' creation


User accessing online service
platform has to verify user age
Self reporting of age
Verifying Age
Profiling (AI/ML)
Collecting behavioural patterns such as facial structure, voice, gait, and keystroke dynamics
Processing
Submission of government ID (e.g., Aadhaar, passport, driver's license)
Verifying ID
User enters credit card information
Information is verified by financial service provider and relayed back
Service provider gets verified age
Service provider initiates age verification
Third party entity such as bank
Child/ Adult
Verifies user's age and relays it back to service provider
Service provider gets verified age
Create personal questions using parent information
Match answers with stored data for authentication
confirm user identity from the answers
Above 18
ACCESS GRANTED
Below 18
Direct child to obtain VPC

The image given below illustrates the different methods of securing VPC.[40]



40 Authors' creation

Self-Declaration: Self-declaration, or "tick box" age assurance, is a common method for age assurance.[41] Users either enter their birthdate or check a box to confirm they meet the age requirement.[42]

However, the language and framing used can encourage more accurate age declarations. For instance, asking "enter your date of birth" instead of "confirm that you are over 18" may prompt users to provide truthful information. If a child submits a date of birth indicating they are above the minimum age, their age can be re-verified later in the process, such as when they log in again ("Can you remind us of your date of birth?"). Children who provided a false date of birth during registration may not remember it when asked later. Any discrepancy can be flagged to a moderator, who may request additional proof of age.[43]

Self-declaration through a check box may not cost much since this can be included in the API development. For example, adding an extra field or pop-up for entering a birthday would take an experienced developer, likely earning around US$75/hr, no more than an hour, to implement.[44]

However, implementing consent or declaration forms can incur annual expenses ranging from US$818[45] to around US$996.[46] The highly scalable method makes it suitable for low-risk use cases and large-scale deployments. However, its reliance on user honesty limits its effectiveness.

---

41 For example, most social media platforms require users to be at least 13 years old to access the service, yet these platforms are still accessible to children. See here: https://www.youthkiawaaz.com/dpdpsurvey/

42 Self-declaration is straightforward for children and suitable for low-risk services, but the way the request is phrased significantly impacts its accuracy. For example, asking for a birthdate is more likely to receive truthful responses compared to simply asking if the user is over 18. This is because the process collects minimal data and is accessible but relies entirely on user honesty, making it highly vulnerable to manipulation, especially by minors trying to access restricted content. Without actual proof of age, it may have limited effectiveness in high-risk situations requiring strict legal compliance. Examples include accessing age-restricted platforms such as purchasing alcohol or tobacco online, engaging with adult content, or participating in financial transactions such as cryptocurrency trading, all of which carry legal and ethical implications for underage users. Available at: https://5rightsfoundation.com/wp-content/uploads/2024/09/But_How_Do_They_Know_It_is_a_Child-1.pdf

43 Ibid

44 https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/6414a45f5001941e519492ff/1679074400513/Privacy+Patchwork+Problem+Report.pdf

45 Online form pricing, https://www.zoho.com/forms/pricing.html

46 Plans and Pricing, https://www.typeform.com/pricing/

Age Estimation (AI/ML): Age estimation techniques use online behaviour patterns to estimate a user's age. These patterns include features like facial structure, voice, gait, and keystroke dynamics, which are analysed through facial scanning and behavioural analysis methods.[47] This raises privacy concerns and has faced criticism for its intrusive nature.[48]

Furthermore, given that Section 9(3) of the Act prohibits behavioural monitoring and tracking aimed at children, such technologies could be restricted. Moreover, Section 9(5) empowers the Central Government to exempt a data fiduciary from the obligations under Section 9(1) if it is satisfied that the data fiduciary processes children's personal data in a manner that is verifiably safe.

Thus, there is a possibility of including such a method under these provisions. The fourth draft rule schedule proposes exemptions to fiduciaries for confirmation that the Data Principal is not a child and for observance of due diligence under rule 10.

The implementation of age estimation systems requires significant investment in infrastructure for data collection, storage, and analysis, making it viable primarily for large-scale platforms only. For instance, established age assurance service providers have invested over US$100mn in platform development. This substantial cost explains why startups, except those explicitly specialising in age assurance, consistently refrain from building proprietary age estimation systems, opting for third-party solutions or simpler alternatives instead.[49]

The cost of integrating third-party applications for age estimation varies depending on the method employed. For example, facial recognition systems are considered one of the most reliable among various age estimation methods. The cost of implementing a facial recognition system varies significantly based on factors such as system type, complexity, and integration requirements. Subscription fees for APIs generally range from US$20 to US$1,000 per month, depending on the volume of transactions and feature set. Integration costs for incorporating facial recognition APIs into existing systems typically start at around US$7,800 and can increase with complexity.[50]

---

47 https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/the-path-forward-minimizing-potential-ramifications-of-online-age-verification/

48 https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/age-assurance-and-age-verification/

49 https://www.yoti.com/wp-content/uploads/Yoti_Overview-2021.pdf

50 https://itrexgroup.com/blog/how-much-does-a-facial-recognition-system-cost/

Developing a custom-built facial recognition system tailored to specific requirements can cost between US$40,000 and US$150,000, with advanced and highly scalable systems potentially exceeding US$500,000. Additionally, hardware costs (e.g., cameras, servers) and ongoing maintenance and retraining expenses add to the total investment. The final cost depends on the specific needs, scale, and level of security required by the user.[51]

A service provider indicated during the consultation that each verification would cost approximately ₹42. The final cost will largely depend on the method being used and additional features, such as the ability to use the exact age estimation across multiple services. Assuming 10,00,000 verifications yearly, the total cost would be approximately ₹42,000,000 (US$494,118). The total cost for a normal system, including API integration, average subscription fees of US$500, and per verification cost, would be US$502,418.

The age estimation process is scalable. However, it can only be developed by larger platforms with significant financial resources and access to large data points.[52] It also poses challenges, including concerns about excessive data collection, surveillance, and the risk of identifying users only after they have already accessed age-inappropriate services.

Continuous data collection could result in highly detailed user profiles, potentially revealing sensitive information such as a child's height, daytime location, interests, closest friends, sexuality, living arrangements, or whether they live in owned or rented accommodation.

This data, once collected, is transferred, processed, and stored for varying periods, increasing its vulnerability to misuse or breaches. It can only deliver limited accuracy in determining specific ages as opposed to broader age ranges. It has also been noted to perform less reliably for people of colour, as well as transgender and disabled individuals, who may disproportionately experience false positives or false negatives.[53]

---

51 https://itrexgroup.com/blog/how-much-does-a-facial-recognition-system-cost/

52 High implementation and operational costs challenge smaller companies, limiting broader adoption.

53 https://www.regulations.gov/comment/FTC-2023-0044-0350

Government-Issued ID Verification: Age assurance using government-issued IDs requires users to provide verified proof of age, such as a photo ID (e.g., Passport and Aadhaar) displaying their date of birth.[54] At a basic level, these systems verify whether an individual's date of birth satisfies predefined age requirements. More advanced systems incorporate authentication protocols and cross-reference identification documents with authoritative databases to ensure validity. The most sophisticated systems integrate biometric analysis to compare real-time facial images (selfies) with the photographs on identification documents, thereby enhancing accuracy and reliability.[55]

The most commonly used government ID in India, Aadhaar costs around ₹0.5 for authentications where only a yes/no response is provided, while Aadhaar e-KYC costs ₹3[56] and for photo-based verification costing ₹15.[57] For 10,00,000 verifications yearly, the annual cost would amount to ₹500,000 (US$5,882), ₹3,000,000 (US$35,294), and ₹15,000,000 (US$176,471), respectively.

While using the government for age verification is relatively accurate, it raises concerns related to security, trust, privacy, and exclusion. For example, it can lead to digital exclusion, especially for children and marginalised groups who lack access to government-issued IDs or digital tools to upload IDs.[58]

Further, this requirement can exclude users who are reluctant to share government-issued IDs, negatively impacting protected speech. Requiring minors to submit government IDs to access digital platforms, such as social media, could exacerbate challenges, as these platforms are integral to their participation in social, economic, and political life.[59]

Smaller, lesser-known companies may struggle to build user trust, as verification steps requiring government ID details can deter users. These companies also face increased

54 https://www.privo.com/blog/what-is-verifiable-parental-consent

55 https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/65d8b6ab876bfd5b70f8795e/1708701355604/FINAL+-+2024+More+Than+Just+A+Number.pdf

56 https://uidai.gov.in/images/Draft_Auth_Pricing_Regulations.pdf

57 https://aadhaarkyc.io/pricing/

58 https://today.umd.edu/umd-analysis-millions-of-americans-dont-have-id-required-to-vote#:~:text=More%20than%2011%20million%20people,unexpired%20government%20issued%20photo%20ID

59 https://online.hbs.edu/blog/post/what-is-a-digital-platform

risks when collecting and storing age verification data. For example, if regulations require startups to prove user ages to regulators, they must store more sensitive personal information. A data breach involving such data could be devastating for an early-stage startup. The average cost per compromised record was US$165, meaning a startup with 20,000 users could incur breach-related costs of US$3.3mn.[60]

In the first half of 2024, the average data breach cost in India was approximately US$2.35mn.[61] Beyond financial repercussions, the resulting business disruption and reputational damage often prove damaging. With limited resources and a focus on revenue-generating initiatives, smaller companies often lack the capital and personnel to invest in developing secondary systems that do not directly support business growth.[62]

The method has limited scalability due to dependency on users having valid IDs and access to digital tools. It can become particularly challenging in resource-constrained areas and for marginalised populations lacking identification documents.

DigiLocker: When a parent is not an existing user of the platform on which the child is trying to access, the draft Rules propose that verification of their age and identity can be done through two pathways. First, the platform may validate parental credentials through a legally authorised entity or government body. Alternatively, the platform can utilise a virtual token system that connects to the parent's voluntarily provided identity and age details, which are securely stored with a digital locker service provider.

For instance, if a child wishes to create a social media account and their parent does not use that platform, the service can verify the parent's credentials through these authorised channels to establish their authority to grant consent for their child's account access. Digilocker's API offers verification at ₹2.99 per verification.[63] With 10,00,000 verifications per year, the total cost would amount to ₹2,990,000 (US$35,176).

60 https://www.ibm.com/reports/data-breach

61 https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec

62 https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/60819983b7f8be1a2a99972d/1619106194054/The+State+of+the+Startup+Ecosystem.pdf

63 https://gridlines.io/products/digilocker

However, it raises privacy, operational concerns, and a lack of clarity on key issues. For instance, while an API could verify age by accessing documents stored in DigiLocker, it would also reveal names, as multiple family members might share the same phone, making it difficult to ensure privacy.[64]

Additionally, relationship mapping through DigiLocker could face challenges, especially in cases involving guardians instead of parents, such as with orphans. Moreover, mandating the use of DigiLocker assumes universal access, posing difficulties for families without the platform or those unwilling to share identification documents.[65]

This approach raises significant privacy concerns, as many users may be reluctant to link their identification with government-authorised mechanisms. Such linkage would eliminate anonymity on digital platforms, undermining users' privacy and online freedom.

Moreover, the Supreme Court of India recently referred to guidelines issued by the Unique Identification Authority of India (UIDAI), clarifying that while the Aadhaar can be used to verify an individual's identity, it is not definitive proof of date of birth. This distinction is significant as many platforms, including DigiLocker, rely heavily on Aadhaar for identity verification and age assurance. The lack of conclusive date-of-birth verification through Aadhaar could complicate the age verification process, creating gaps in compliance with age-related regulations.[66]

Third-party verification: Third-party verification offers a streamlined approach to age and parental consent verification across different platforms. In this system, users submit their verification requests through an intermediary service with an established relationship. This approach is particularly valuable when parents and children use different platforms, eliminating the need for both to be present on the same service. The process typically begins with users providing identity documents (like passport scans) and facial images to the third-party provider for initial verification. Once verified,

64 https://www.hindustantimes.com/india-news/govt-may-define-specific-steps-for-parental-control-measures-101721331151567.html

65 https://www.hindustantimes.com/india-news/govt-may-define-specific-steps-for-parental-control-measures-101721331151567.html

66 https://www.hindustantimes.com/cities/bhopal-news/aadhaar-card-is-not-proof-of-age-only-identity-reiterates-madhya-pradesh-high-court-101731342670915.html

this system eliminates the need for users to repeatedly submit official documents across multiple platforms, making the verification process more efficient.[67]

Third-party providers charge approximately ₹20 per verification, with an additional monthly fee of around ₹2,100 (US$24.5 and a conversion rate of US$1 = ₹85). Assuming an average of 10,00,000 verifications annually, this results in a yearly cost of ₹20,000,000 (US$235,294) and ₹25,200 (US$294) annual additional fee, totalling US$245,554. 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.

It has the potential to reduce the sharing of personal data and give users more control over the specific attributes of their identity. However, it may also reveal more information than necessary to prove a user's age.[68]

Likewise, if they upload a passport scan or selfie, they may not know that their data is being analysed, shared, or stored by a third party. While users, including children, may have technically agreed to this through terms and conditions or privacy notices, they are often unaware of how their data is being processed and shared, violating data minimisation and purpose limitation.[69]

However, the method may unintentionally expose more information than necessary. For example, uploading passport scans or selfies may involve third-party analysis, storage, or sharing of personal data. Often, users may technically consent to this through terms and conditions or privacy policies yet remain unaware of how their data is processed. These practices risk violating core data protection principles such as data minimisation and purpose limitation.

It may also involve sharing user information with external entities, raising privacy concerns and increasing the risk of liability in the event of data breaches and manipulations. Scaling these systems poses challenges, primarily because no integrated API exists across providers. The use of diverse technologies and differing standards further complicate the process. These costs pose particular challenges for

---

67 https://www.dock.io/post/reusable-identity

68 https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/the-path-forward-minimizing-potential-ramifications-of-online-age-verification/

69 See this: Identity Verification, OnlyFans Privacy Policy. Available at: https://onlyfans.com/privacy

small-scale companies. As these companies typically operate at a loss while building toward scale, additional operational expense directly reduces their financial runway, effectively shortening the timeframe they have to achieve sustainability.[70]

Credit Card: An adult, typically a parent or legal guardian, can verify a child's age or age range, as many forms of identification, such as credit cards, are generally available only to adults.[71] In this approach, the adult provides the child's information and consent, unlike previous methods where the child's age is first established, and the adult's role is limited to giving consent afterwards. This process makes it easier for adults to verify their age than for children. For card-based verification, service providers charge around ₹0.45 per verification,[72] leading to a yearly cost of ₹450,000 (US$5,294) for 10,00,000 verifications.

However, minors with access to payment methods, such as prepaid cards, credit cards or parent-linked accounts, can bypass restrictions designed to enforce age verification. This approach also creates financial barriers for families without access to credit cards or online payment systems, further excluding them.

Credit card penetration in India is around 100 million, or 7 percent of the population[73] which can exclude the economically disadvantaged. Fiduciaries may need to adopt alternative methods for those without access to cards. Requiring sensitive financial information on potentially unsecured platforms raises security risks, further complicating its viability as a robust age verification method.

---

70 Given the heavy investment around VPC, smaller companies may frequently resort to third-party verification vendors. The integration of external verification systems typically demands a significant investment, potentially reaching millions of Indian rupees, and requires weeks of development time. While outsourcing verification to established providers may enhance user trust, it does not eliminate the fundamental concerns regarding time investment and privacy invasion that often deter potential users. The financial implications of third-party verification services manifest in pricing models, ranging from per-verification charges of thousands and thousands of rupees. Available at: https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/61b26e51cdb21375a31d312f/1639083602320/Startups%2C+Content+Moderation%2C+and+Section+230+2021.pdf; https://slashdot.org/software/age-verification/#:~:text=On%20the%20lower%20end%2C%20you,facial%20recognition%20or%20biometric%20authentication

71 https://www.rblbank.com/blog/banking/credit-card/know-the-eligibility-criteria-applicable-for-a-credit-card?srsltid=AfmBOorPMjDQ-P_hF3VxcU0Kphg8yZZC2BdS5QHdGIvPRKPMKnVCE8_6

72 https://www.verifymyage.co.uk/pricing; https://pure.strath.ac.uk/ws/portalfiles/portal/142093023/AgeVerification.pdf

73 RBI data | Finance News—Business Standard shows that credit cards breach the 100 million mark in India,

Knowledge-Based Assessment (KBA): KBA involves asking users questions that only they would know the answers to based on their personal information or knowledge. This is done using challenge questions.[74]

In the context of age verification, KBA can serve as an essential tool to ensure that the person using a service is over 18. For example, a platform may ask a set of KBA questions that pertain to personal information the parent has shared, such as their childhood name or the parent's own past contact details. This helps confirm that the user is over 18.[75] There are also ways in which a customer service representative can ask consumers to answer some randomly generated questions to authenticate their identity and age.[76]

KBA software must generate and manage personalised challenge questions for each parent. Depending on the provider, the pricing ranges from approximately US$1 to US$5 per KBA attempt.[77] Assuming that the cost per verification decreases with an increase in verifications and is US$0.8 per attempt, the yearly fee for 10,00,000 verifications would amount to US$800,000. The cost is expected to decrease significantly when distributed across a large user base. However, startups and services catering to niche groups, such as athletes, may face challenges due to their smaller user base.

However, research indicates that up to 30 percent of legitimate customers struggle with KBA questions, leading to increased call durations and higher operational costs. Conversely, more than half of fraudsters can successfully navigate these questions, undermining security efforts.[78]

The average call duration in contact centres has increased by almost two minutes, with the cost per call rising by up to 40 percent over recent years. The cost to authenticate callers has also increased by US$0.22 per call. These inefficiencies contribute to customer dissatisfaction, with false reject rates reported as high as 25 percent in some cases, resulting in unacceptable levels of customer dissatisfaction. While these figures are derived from other jurisdictions, the likelihood of higher costs and rejection rates

---

74 https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-seeks-public-comment-imperium-llc-proposal-parental-verification-method-under-coppa-rule/130909imperiumapplication.pdf

75 https://withpersona.com/identity-glossary/knowledge-based-authentication-kba

76 https://www.pindrop.com/blog/the-true-costs-of-knowledge-based-authentication-questions

77 What Is KBA (Knowledge-Based Authentication) And How Much It Will Cost You in 2022 - Blog

78 https://www.pindrop.com/blog/the-true-costs-of-knowledge-based-authentication-questions

in India is even greater due to socio-economic and educational barriers, making KBA a less reliable verification method in such contexts.

Furthermore, the persistence of KBA, despite its declining effectiveness, can lead to increased customer attrition, revenue churn, and loss of brand reputation. Transitioning to more secure and efficient authentication methods, such as voice biometrics, has been shown to reduce false reject rates to less than 3 percent, enhancing both security and customer satisfaction.[79]

The method also requires processing parents' sensitive personal data, such as past addresses or phone numbers, raising privacy concerns. Many parents may hesitate to share such information on unfamiliar platforms, highlighting the need for clear and transparent data policies.[80]

While KBA avoids the need for additional hardware or documentation, it relies on accurate recall of specific details, which can frustrate users if questions are ambiguous or data records are inaccurate. Its moderate accuracy stems from effectively validating known information, but overly generic questions may allow unauthorised access.[81]

Scalability is feasible for platforms with moderate user bases due to real-time automation, but high implementation costs per attempt limit its practicality for larger-scale operations. This is due to the need for continuous updates of question databases and the assurance of data accuracy and security. Additionally, maintaining performance and response times requires investment in infrastructure and support, making overall costs include both per-attempt fees and the necessary resources for scaling.

For Registered Parents: When a child initiates account creation, the draft Rules propose that platforms may utilise existing verified parental data within their system to streamline the verifiable parental consent process. If a parent is already a user of the platform with verified credentials, the process begins with the minor entering their age during signup. The platform then pauses the registration and requests the parent's username. Upon receiving the username, the platform can reference the parent's previously verified age and identity information to validate their authority. The parent

79 Ibid

80 https://fpf.org/wp-content/uploads/2023/06/FPF-VPC-White-Paper-06-02-23-final2.pdf

81 Ibid

receives a comprehensive notification detailing their child's requested permissions, including what data will be collected and how it will be used.

Using their existing account credentials, the parent can review this information and decide to approve or deny their child's account request. This process incurs costs related to searching usernames in the database and sending emails, texts, consent pop-ups or making video calls to obtain verifiable parental consent, as outlined in the relevant sections.

Email-based Consent System: When a minor tries to create an account, the platform requests a parent's email. A verification link is then sent to the parent's email, detailing the service, what the child will access, and how their data will be used. Parents must click the link and complete a consent form, providing basic information to confirm their identity.[82]

Standard email prices range from ₹5,333[83] to ₹38,500[84] per month, resulting in approximately US$753.6 and US$5,435 annual costs, respectively. Drafting a comprehensive consent form using a third-party service can cost ₹69,600[85] to ₹83,604[86] annually (approximately US$752 to US$5,429). Totalling these costs leads to a range of US$1,505.6 to US$10,864.

This method offers convenience because it relies on a familiar communication channel, making it broadly usable. However, while easy to implement and widely accessible, it has vulnerabilities. Tech-savvy minors can create temporary emails or access their parents' accounts to bypass verification. Some platforms mitigate this by adding checks like domain age verification or requiring professional email addresses. Further, the system remains susceptible to fraud, as miscreants can mimic official platform emails to deceive users.

It also heavily depends on the data collected during verification, including the parent's email and personal information, which can raise privacy concerns if data safeguards are insufficient. Furthermore, this can also be labour-intensive, time-consuming,

82 https://www.adobe.com/acrobat/hub/what-to-know-about-parental-consent-forms.html

83 Gmass Pricing, https://www.gmass.co/pricing

84' Marketing Pricing' (*Mailchimp*) < https://mailchimp.com/pricing/marketing/ > accessed June 06, 2024.

85 Online form pricing, https://www.zoho.com/forms/pricing.html 5800*12, accessed September 03, 2024

86 Supra Note 45

inconvenient for parents, and costly to implement.[87] Scalability in email-based parental consent systems requires optimised delivery and error handling to manage high volumes efficiently, increasing costs.

Video Identification Mechanism: Video verification requires parents to record and submit a short video statement stating their name and their child's name, giving explicit consent for the service, showing their face, and showing a valid ID. Trained staff review the videos to confirm authenticity, verify identity, and ensure the consent meets legal requirements.[88]

Video conferencing software like Zoom Enterprise costs ₹21,600 (US$251.96) per year.[89] Other third-party service providers charge amounts ranging from €0.85 (approximately US$ 0.11)[90] to around 45p (approximately US$0.57)[91] per verification. Many providers offer subscription-based pricing, typically costing around US$49 per month.[92] The yearly cost for 10,00,000 annual verifications can vary, ranging from ₹110,000 (US$1,294) to ₹5,700,000 (US$67,059).

While this method provides strong verification, since its accuracy is due to real-time identity checks that minimise circumvention risks, it does have some issues. By requiring parents to come on a video call, the platforms may have access to personally identifiable information such as facial data, hence raising privacy concerns, particularly for individuals valuing anonymity. Thus, the invasive nature of video verification may deter participation.

From a convenience standpoint, the process is time-intensive and demands technical literacy, making it less accessible to parents with limited digital skills or in urgent situations. Moreover, scalability remains a critical issue, as handling high volumes of video submissions is resource-intensive for platforms with large user bases. Adding resources, staffing, and infrastructure increases costs, limiting its feasibility for

87 Supra Note 79

88 https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/age-assurance-and-age-verification/

89 https://zoom.us/pricing

90 https://ondato.com/plans-pricing/

91 https://www.verifymyage.co.uk/pricing; https://pure.strath.ac.uk/ws/portalfiles/portal/142093023/AgeVerification.pdf

92 https://www.veriff.com/plans/self-serve

widespread adoption.[93] Higher call volumes may also require software upgrades, such as AI-enabled verification processes or enhanced infrastructure, which can be costly at larger scales.

SMS Verification System: SMS verification begins when the platform sends an SMS notification to the parent or legal guardian if the parent has already registered with the platform. The message informs the parent about the child's attempted login and the requirement for parental consent. The system sends a one-time password (OTP) to the number, which the parent must enter within a specified time (usually 1-2 minutes).[94] The standard prices for SMS can cost around ₹16,500 for around 1,00,000 SMS.[95] With 10,00,000 verifications per year, the yearly cost would be ₹165,000 (US$1,941).

Since this method requires only a phone number for validation, it offers some privacy protection by avoiding collecting additional personal details. Its simplicity and speed make SMS verification highly convenient, as most parents have access to mobile phones, although it may be less accessible for those unfamiliar with technology. With a robust SMS infrastructure and widespread availability of SMS services, this method can effectively scale to accommodate large user bases.
However, the possibility of children accessing a parent's phone and sharing verification codes also introduces risks of circumvention and accuracy. Additionally, the FTC has denied the use of mobile phones for VPC collection, as it is difficult to verify that the parent or guardian is providing consent.[96] However, this can be mitigated with dual-factor authentication, combining SMS with other methods, which may make it more inconvenient.[97]

Operating System/App Stores: Many devices and operating systems offer controls to create age-appropriate digital experiences for children. They can be applied at the system or device level, enabling features like "child mode" to adjust services and

93 https://edri.org/wp-content/uploads/2023/10/Online-age-verification-and-childrens-rights-EDRi-position-paper.pdf

94 What Is SMS OTP? Benefits, Implementation and Use Cases

95 https://2factor.in/v3/bulk-sms-pricing

96 Supra Note 79

97 *Ibid*

content by default. Platforms like Apple,[98] Google[99] and others allow the creation of family accounts where parents can add child profiles.

Further, they also have age and content ratings for apps and games that help users, especially parents, determine the suitability of apps for different age groups based on their content and are used for putting these parental controls. The parent then manages the child's account settings, including privacy controls. For example, Apple's "Ask to Buy" feature allows parents to approve or deny app purchases from their child's device.[100] Additionally, parents can revoke consent at any time, which will immediately render the app unusable on the child's device.[101]

Platforms like Google Play and Apple's App Store already charge commission fees ranging from 15 to 30 percent of app revenue from in-app purchases. These fees cover services such as app hosting, developer tools, and other resources.[102]

If a company generates ₹10,00,000 (around US$11,764) annually from in-app purchases, the commission could range from ₹1,50,000 to ₹3,00,000 (US$1,764 to US$3,529) annually. There's also a one-time US$25 registration fee for the developer account on the Google Play Store, while there's an annual fee of US$99 for the Apple Developer Programme.[103] This comes to the total cost range for using the Apple App Store, from US$1,863 to US$3,628 annually. These platforms also have already established age ratings for apps.[104]

Embedding the consent process within the app store infrastructure can improve efficiency and reduce costs by eliminating the need for additional software development. Familiar app store interfaces enhance user trust and make setup straightforward. Scalability is a key strength, as these systems integrate seamlessly across multiple devices and family profiles.[105]

---

98 Use Family Sharing to provide parental consent for your child's existing Apple Account

99 Provide consent & add supervision to your child's Google Account - Google For Families Help

100 Approve what kids buy with Ask to Buy - Apple Support (IN).

101 Use parental controls on your child's iPhone and iPad – Apple Support (IN)

102 Service fees - Play Console Help, Every Apple App Store fee, explained: How much, for what, and when | AppleInsider

103 https://appradar.com/blog/google-play-apple-app-store-fees

104 *Ibid*

105 The Kids Online Safety Act Was a Good Start, But App Stores Need Accountability Too | Institute for Family Studies

However, accuracy depends heavily on the robustness of age restrictions and content filters, which may require ongoing parental supervision to address gaps. This can be due to account sharing, children bypassing restrictions, or content misclassification.

Reliance on app store policies and guidelines can limit flexibility, as developers must conform to predefined Rules set by platforms.[106] Furthermore, heavy dependence on dominant platforms like iOS and Android raises competition concerns, as it risks reinforcing their market power and stifling innovation from smaller platforms or alternative systems.[107]

Zero Knowledge Proof (ZKP): ZKP is a cryptographic approach that verifies a parent's consent to collect and process their child's data without revealing personal details.[108] They use cryptographic protocols to prove they meet the conditions for consent. This includes demonstrating their age and relationship to the child. The process ensures that sensitive information, such as the parent's identity or age, is kept private. The output of this process is a hashed value, referred to as a "proof statement," which serves as verification without disclosing any actual personal details. The cryptographic proof generated by the parent is securely transmitted to the service provider. This proof confirms that the parent can provide consent without revealing sensitive data. It serves as confirmation that the consent is legitimate while ensuring privacy.

Upon receiving the proof, the service provider validates it using a verification key provided by the third-party entity. If the evidence is successfully verified, the service provider acknowledges and logs the consent for compliance.[109]

The service provider stores no personal information, ensuring privacy and compliance with data protection regulations. In line with the draft Rules, the UIDAI could implement an age verification system by generating tokens for Aadhaar holders that verify if a user meets age requirements when processed through Zero-Knowledge Proof protocols. This system would function similarly to virtual IDs, with users generating tokens through the UIDAI website. These tokens would enable age-

106 App stores, antitrust, and their links to net neutrality: A review of the European policy and academic debate leading to the EU Digital Markets Act.

107 https://assets.publishing.service.gov.uk/media/62a0d1b68fa8f5039b2078e5/Appendix_H_-_In-app_purchase_Rules_in_Apples_and_Googles_app_stores.pdf

108 https://exmachina.in/10/04/2024/age-tokens/

109 https://www.leegality.com/consent-blog/child-consent

appropriate access to digital services while protecting user privacy by withholding other personal information.[110]

The total cost for hardware and configuration is estimated at US$15,640, including processing power, memory, hardware, and installation expenses. This does not include the infrastructure cost discussed above since the method consists of development for cryptographic processing. The additional infrastructure and installation required amounts to approximately 50 percent of the cost of purchasing and setting up the hardware. This adds US$7,820 to the hardware and configuration costs, resulting in an estimated total upfront investment of US$23,640. The cost of verifying one Zero-Knowledge Proof (ZKP) is approximately US$0.226.[111] This results in a yearly verification cost of ₹2,260,000 (US$26,588) for 10,00,000 verifications.

The costs of developing and implementing ZKP solutions can be substantial, as also demonstrated by investments, such as US$5mn in specialised chips aimed at reducing ZKP costs.[112] This level of investment in advanced computation resources underscores the financial barriers smaller players and startups may face when attempting to develop or adopt ZKP solutions. The need for specialised hardware and significant computational resources makes it difficult for smaller organisations to compete.[113]

110 https://www.livemint.com/opinion/online-views/aadhaarbased-age-tokens-can-solve-a-privacy-problem-11712663231351.html

111 ZK Prediction: USD 0.12 market price per ZK proof in 2030 (part 2) | by ZKWispr.

112 https://cryptobriefing.com/polygon-zero-knowledge-investment/?utm_source=chatgpt.com

113 Using cryptographic proofs instead of raw data, ZKP ensures personal details remain undisclosed. This reduces risks such as identity theft. However, its effectiveness depends on third-party verifiers' reliability and cryptographic algorithms' integrity. Trusted verifiers must handle and encrypt user data, posing privacy risks if compromised. ZKP is scalable through decentralised systems like blockchain, which reduces reliance on centralised databases. However, its resource-intensive processes and technical expertise requirements hinder widespread adoption among non-technical users. Managing increased computational loads as user numbers grow adds complexity, slowing performance and raising infrastructure costs. These scalability challenges and high operational expenses highlight the financial barriers to adopting ZKP, particularly for organisations with limited resources. Available at: https://ifstudies.org/ifs-admin/resources/briefs/ifs-eppc-ageverificationpolicybrief.pdf

4 Conclusion and Recommendations

Conclusion

The debate over VPC underscores the need to balance protecting children and preserving online freedom. While the government and platforms must safeguard minors from harmful content and data abuse, VPC presents multi-layered challenges. The government's prescribed approaches in the DPDP draft Rules — such as using existing platform data or authorised government entities like Digital Locker services — may not be optimal in terms of security, cost, and efficiency.

These methods come with varying costs, privacy, and effectiveness concerns and may inadvertently harm the children they aim to protect. They also change the open nature of the internet and user interactions. Age restrictions work well in specific areas where regulations are clearly defined. The cost incurred by implementing VPC mechanisms should be proportional to the benefits they provide.

It may not justify sharing sensitive information for access to content that poses minimal harm to teenagers. The choice of VPC tools should depend on the level of risk to children and the associated cost of the mechanism, ensuring a balanced and appropriate approach. Any VPC system involves trade-offs, and it falls to policymakers and service providers to determine which compromises are acceptable, including privacy, security, and convenience, as well as the creation of costs and compliance burdens. These considerations are particularly important as smaller companies, operating with limited resources, are competing with globally established platforms and must balance regulatory compliance of VPC with maintaining market competitiveness.

Most parents support their children's internet use, with 80 percent stating that it significantly helps their children acquire knowledge.[114] Digital platforms handling children's personal data may frequently need to seek parental consent, which can increase operational costs due to the added time and resources required.[115]

[114] Ibid

[115] Supra Note 79

This could disproportionately affect smaller platforms, as it raises their customer acquisition costs and strains their capacity to manage ongoing compliance. Children may have to seek permission from their parents, making the process tedious and discouraging their engagement with digital platforms. This could lead to frustration for both parents and children, negatively impacting their experience.[116]

Moreover, such mandates may negatively impact innovation, as service providers may become reluctant to invest in new services for minors due to the added compliance burden.

The situation is further complicated by India's significant digital divide, where varying levels of technology access and digital literacy create additional barriers to effective implementation. The parental consent requirement poses particular challenges in the Indian context. Many parents lack the digital skills necessary to navigate online consent mechanisms effectively, potentially limiting their children's access to valuable digital resources and educational opportunities. This disparity in digital literacy may widen existing social and educational gaps, as children from digitally literate households may gain easier access to online resources compared to families with limited digital exposure.

The development of VPC should be shaped not just by government regulations but also by innovation and the cost implications for the broader ecosystem. Instead of mandating specific verification channels, the draft Rules should allow platforms to implement solutions that align with their technical capabilities and user needs.

A market-driven approach, where platforms can choose and transparently disclose their verification methods, would enable parents to make informed decisions about which platforms best protect their children while respecting their preferences. This competition would drive innovation, leading to more efficient, user-friendly solutions. Such flexibility would be particularly valuable for smaller platforms, allowing them to choose cost-effective solutions without compromising security. In comparison, larger platforms could adopt more comprehensive systems based on their resources and user base.

Policymakers should consider establishing risk-based Rules rather than being prescriptive, allowing room for innovation and enabling the identification of effective

[116] https://www.youthkiawaaz.com/dpdpsurvey/

methods in different contexts, along with considering the use case and the age of the user. To achieve the shared goal of a digital world that accounts for children's varying ages and capacities, a mixed approach to age assurance methods should be adopted. These methods must be privacy-preserving, transparent, accountable, scalable and suitable for the specific context in which they are used. They should be designed based on agreed-upon standards that service providers can implement and regulators can enforce, with oversight from civil society and consumer groups, to ensure compliance and effectiveness.

Recommendations

Adopting a Non-Prescriptive Approach: The draft DPDP Rules could avoid specifying particular approaches to age assurance, methods, data sources, or technical solutions in order to reduce compliance costs, especially for smaller platforms. As it is clear from the above discussion, each VPC method has its benefits and challenges. Thus, service providers should be allowed to implement verification methods that align with their specific context, considering three primary factors: the nature of the use case, the level of associated risks, and the scope of implementation costs, both direct and indirect. This recognises a spectrum of risk levels that warrant different verification standards.

For lower-risk activities, such as accessing general information, viewing non-sensitive content, or engaging in fundamental user interactions like writing product reviews, simpler verification methods, including self-declaration, may be appropriate. In contrast, high-risk activities, including access to age-restricted content such as alcohol and financial transactions, necessitate more robust VPC methods, such as government-issued document-based verification.

Further, the VPC process should incorporate both initial and ongoing assessment methods. When users register for a service, their declared age serves as a baseline, but their subsequent patterns may trigger additional verification requirements.

For example, suppose a user claiming to be 16 years old displays sustained engagement with content typically associated with younger audiences, such as children's entertainment or games. In that case, the system should flag this discrepancy for moderator review and require additional age verification, like a government-issued ID.

Services should implement a precautionary approach by designing their age-appropriate safeguards to protect the youngest users within their stated age range. This ensures that content and interactions remain suitable for all users while maintaining appropriate safety standards. Through this non-prescriptive risk-based framework, regulations can achieve their protective aims without imposing unnecessary burdens on service providers or users.

Establishing an Independent Assessment Group: We also recommend establishing an independent assessment group by bringing together consumer groups, technical experts, and child development specialists to balance innovation with protection. The group can develop codes and standards, suggest mechanisms to pool resources for small businesses, manage grievances, and resolve disputes. These standards would establish baseline requirements for service providers while remaining adaptable to technological advances.

Such a baseline would recommend ways to handle user information responsibly, focusing on data protection principles, including limited data collection, prevention of unauthorised retention, restrictions on biometric data processing, and preservation of user anonymity where appropriate. The group could also review the implementation of VPC after a specified period to assess its effectiveness in protecting children's data protection. This review would help identify concerns, challenges, and risks while exploring mitigation strategies to enhance its efficiency. It would also provide an opportunity to evaluate the overall utility of VPC and consider alternative approaches for better online child protection.

Beyond its independent assessment function, the group would act as an educational resource, providing guidance to policymakers, service providers, startups, parents, and guardians about available VPC methods, their associated risks, costs, use cases, and less intrusive alternatives. This educational component would help stakeholders make informed decisions about VPC and ensure that protective measures remain proportional to identified risks.[117]

The group would consult regularly with these key stakeholders and ensure that safety, privacy, and accessibility considerations remain central to system design and implementation.

[117] Supra Note 92

Interoperable Verifiable Parental Consent Framework: We recommend implementing an interoperable verifiable parental consent framework across digital platforms. Similar to the telecommunications sector, where different service providers communicate seamlessly, or the payments sector, where transactions between different banks and wallets are allowed, platforms should be permitted to establish secure protocols for sharing verified parental consent. This would ease compliance burdens, improve efficiency, and minimise data collection. Standardised protocols should enable secure communication of consent queries and responses while ensuring data protection.

Suppose a parent has already been verified on one platform, and their child wishes to use another platform where the parent is not registered. In that case, the minor should be able to direct the new platform to communicate with the platform the parent is using (and has verified their identity) to obtain their decision on whether or not to allow the child to access the new platform. This would enable seamless communication between platforms, simplifying verification and conveying consent. Parents would only need to verify once, reducing barriers to digital participation, especially in regions with limited access to government ID services, digital infrastructure, or digital literacy. The framework must establish clear limits on what data (which must relate only about parent's decision) can be transferred between platforms.

It may be argued that rule 10(1)(a) of the Draft Rules technically do not curb communication between platforms and allow one platform to collect parental data (reliable details of identity and age of the parent) from another, through valid consent of parent. However, this approach can create unnecessary privacy and security risks, as a set of data (parent's details) would be duplicated and travel from one platform to another. Moreover, such data duplication will not benefit a parent if they never intended to use the platform which the child seeks to acces. A better approach would be to prescribe a narrow communication protocol, where if a platform has already verified a parent's identity and age, another platform can simply initiate communication to obtain consent. This streamlined approach would make the process more accessible, minimise repeated submission of sensitive data, and protect privacy by limiting transfers.

To ensure security and accountability, platforms in the interoperable framework should follow strict technical standards and reporting requirements, ensuring convenience does not compromise child protection.

CUTS International

D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India
Ph: 91.141.228 2821, Fax: 91.141.228 2485
Email: cuts1@cuts.org, Website: www.cuts-international.org

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