Age Verification Methods and Privacy: Online Anonymity of Children and Adults

Dallin M. King

Brigham Young University

WRTG 316: Technical Communication

Abstract

This literature review examines age verification (AV) methods for protecting children's and adults' digital privacy, with a focus on the central research question: How do current internet age verification methods affect the privacy and anonymity of children and adults? Regulatory efforts to protect minors from explicit content have prompted a shift from privacy-preserving, low-assurance methods such as self-declaration to more data-intensive, high-assurance systems. Five primary AV methods (self-declaration, identification-based verification, biometric verification, age estimation, and attribute-based verification) are analyzed. These methods were selected based on their current prevalence across regulatory frameworks and digital platforms, their focus in recent legislation, and their technological maturity as identified in the literature. Current legal and technological interventions introduce significant new risks. High-assurance approaches require ongoing collection of sensitive personally identifiable information (PII) or physiological data. This reduces online anonymity and increases the risk of data aggregation. These systems may reinforce demographic biases and are often circumvented by technologically adept youth. Decentralized attribute-based verification offers a potential privacy-preserving alternative, but its adoption is limited by market constraints and user distrust. AV mandates can compromise digital security. Further research is needed to develop transparent, user-centered age-assurance technologies that address deficiencies in privacy literacy.

Keywords: *age verification, digital privacy, online anonymity, children, adults, personally identifiable information, biometric verification, self-declaration, data security, legislative compliance, youth rights.*

Age Verification Methods and Privacy: Online Anonymity of Children and Adults

Lawmakers advocate for robust age verification (AV) systems in response to the increase in internet use (Abdulla, 2025; Jarvie & Renaud, 2024; Murray et al., 2025). These efforts, such as the United Kingdom's Online Safety Act and recent U.S. laws, aim to protect minors from accessing Sexually Explicit Media (SEM) (Woodley et al., 2025; Murray et al., 2025). As a result, AV approaches have shifted from privacy-oriented, low-assurance methods to more data-intensive systems. This transition is motivated by a desire for greater compliance and effectiveness, but reliance on so-called "techno-legal solutionism" introduces additional risks (Angel & Boyd, 2024).

These AV systems are designed to better protect children, yet they foster a shift towards high-assurance verification methods and away from simple self-declaration (Pasquale et al., 2022). This transition results from demands to improve accuracy and compliance, which increases the collection of sensitive personal information and biometric data (Murray et al., 2025; Stardust et al., 2024). While these measures are intended to strengthen safeguards for minors, they simultaneously affect user anonymity and privacy across all demographics.

For adults, diminished anonymity undermines civil liberties and discourages lawful access to sensitive information. It also increases data security risks and the aggregation of AV data by creating attractive targets for cyberattacks. This elevates the risk of identity theft, increases minors' vulnerability, and diminishes privacy (Murray et al., 2025; Yar, 2020). Additionally, AV mechanisms normalize corporate "dataveillance," which involves corporations tracking children (Crepax et al., 2022). Stringent parental consent and oversight requirements reduce adolescents' "internal privacy" and autonomy, both of which are essential for safe access to educational resources and support. (Abdulla, 2025). These privacy trade-offs are worsened by evidence that technologically skilled youth can circumvent AV measures by using Virtual Private Networks (VPNs), calling into question the overall effectiveness of these measures (Turvey et al., 2024; Woodley et al., 2025; Yar, 2020). The debate extends to children's rights. Some scholars advocate for greater youth political influence over relevant legislation (Woodley et al., 2025;

Bowler, 2026); others contend that online environments should mirror offline age restrictions (Murray et al., 2025).

This literature review is organized around the central research question: How do current internet-age verification methods affect the digital privacy and anonymity of children and adults? Specifically, it examines AV methods that are intended to protect vulnerable populations but also compromise users' digital security and anonymity. To address this question, the review analyzes the primary AV methods: self-declaration, identity-based, biometric, age estimation, and attribute-based verification.

Self-Declaration

Self-declaration is the most basic age verification (AV) method. In this approach, users confirm their age by selecting a checkbox or entering a birthdate during registration. This method is highly accessible, but it highlights the tension between privacy and restricting minors' access to adult content.

From a privacy perspective, self-declaration is desirable because it minimizes the collection of personally identifiable information (PII). This minimization preserves the digital anonymity of both children and adults. Although the low-friction nature benefits platforms and researchers, it isn't protective. Henderson et al. (2012) emphasize the risk of falsification and fraudulent completion. They note that minors can easily misrepresent their age to gain access without detection. Hence, researchers characterize self-declaration mechanisms as a form of "security theater" rather than a robust protective safeguard (Jarvie & Renaud, 2024). Overall, while self-declaration offers substantial privacy benefits and ease of use, its susceptibility to falsification and the lack of reliable enforcement make it the least effective option for strict compliance or protection from explicit adult content.

In contrast, reliance on self-declaration is central to a broader legal and ethical debate over minors' rights and capacity to consent online. On the one hand, regulations like the US Children's Online Privacy Protection Act (COPPA) and the EU's General Data Protection Regulation (GDPR) establish a strict "digital age of consent", typically between 13 and 16, based on the premise that children lack the cognitive maturity to consent to data processing or exposure to adult content (Pasquale et al., 2020; van

der Hof & Ouburg, 2022). Advocates argue that digital environments should mirror real-world age restrictions; thus, self-declaration is inadequate because it allows children to bypass parental oversight, prompting some to advocate for more rigorous barriers.

However, human rights scholars and privacy advocates contend that self-declaration is the only method that balances protection with the youth's evolving capacities. Stardust et al. (2024) argue that a restricted-access scheme based on a simple yes/no question about a user's age is beneficial. This low-friction approach minimizes accidental exposure while enabling users to make intentional decisions about consent. Additionally, self-declaration protects what Abdulla (2025) describes as a youth's "internal privacy", defined as autonomy from parental and corporate surveillance. For marginalized adolescents or those in abusive environments, the ability to anonymously self-declare readiness to access educational or sexual health resources is considered a vital digital right that invasive AV methods would undermine (Abdulla, 2025).

In conclusion, self-declaration is a low-assurance method. However, as scholars and policymakers continue to debate the digital age of consent, this approach could easily resurface. More research is required on youth rights, autonomy, and their capacity for digital consent to fully understand how to balance protection and privacy. As a result, self-declaration remains a viable option, actively contending for a position in the broader landscape of age verification.

Identification-Based Verification

Identification-based verification uses "hard identifiers," such as government-issued documents or credit cards, to verify a user's age. Unlike self-declaration, this approach prioritizes legal compliance over digital privacy and anonymity.

The effectiveness of identification-based methods varies. Hokke et al. (2018) reference a 2007 study by Fox et al., which found that "postal consent," requiring physical documents to be mailed, resulted in low return rates because the process is expensive and labor-intensive. In contrast, Henderson et al. (2012) support telephone verification, which allows direct interaction between researchers and parents

to more accurately confirm a child's age. However, Yar (2020) and Woodley et al. (2025) observe that minors can circumvent these systems by using parents' credit cards or IDs without permission or by obtaining fake documents. Additionally, Murray et al. (2025) report that strict identification requirements prompt users to use Virtual Private Networks (VPNs) or access unregulated websites to avoid identification, thereby increasing exposure to cybersecurity risks.

In the context of privacy, research shows conflicting perspectives among parents, privacy advocates, cybersecurity scholars, and adolescents. Abdulla (2025) observes that certain parents are willing to accept privacy trade-offs, such as submitting Social Security Numbers, to enhance children's online safety. However, this parental viewpoint contrasts with the concerns raised by privacy advocates and cybersecurity experts, who emphasize the systemic risks posed by the collection of personally identifiable information (PII). Murray et al. (2025) and Yar (2020) argue that such practices dissolve online anonymity by tying users' real-world identities to their digital behavior. In addition, both privacy advocates and adolescents warn that centralized repositories of hard identifiers are high-value targets for cyber-attacks. As Murray et al. (2025), Yar (2020), and Woodley et al. (2025) collectively illustrate, data breaches involving these identifiers yield far-reaching consequences, including identity theft, extortion, and reputational damage. This debate over the perceived safety gains and the substantial risks they introduce is ongoing, and further research is needed to understand people's perceptions of risk and its weight.

Further, scholars examine the exclusionary effects of identification-based methods across socioeconomic groups. While privileged users can verify their age, Stardust et al. (2024) and Yar (2020) emphasize that reliance on credit cards or official IDs discriminates against marginalized adults, undocumented individuals, and economically disadvantaged populations who lack access to credit-based financial services. Livingstone et al. (2024) reinforce this distinction, noting that data protection authorities view hard identifiers as a privacy violation, requiring more personal data than necessary, and unjustly exclude minority populations.

In summary, identification-based verification legally complies with regulatory requirements; however, the weight of user-perceived privacy and accuracy isn't widely studied. While identification-based verification meets more rigorous gatekeeping standards, the literature shows that it undermines digital anonymity, intensifies socioeconomic exclusion, and increases the risk of data breaches. In addition, the research shows that these systems are easily circumvented by the children it aims to protect.

Biometric Age: Verification and Estimation

Biometric age assurance is regarded as the most advanced technological approach in internet regulation, yet it raises significant privacy and ethical concerns. These technologies are typically categorized into biometric verification and age estimation. Biometric verification provides high-assurance identity confirmation by matching users to established records using permanent physiological characteristics, such as facial geometry, fingerprints, or iris patterns (Pasquale et al., 2020). In contrast, age estimation employs probabilistic artificial intelligence (AI) to predict an individual's age group based on behavioral profiling, including digital traces, gesture patterns, and browsing history (Crepax et al., 2022; Livingstone et al., 2024; Stardust et al., 2024). Although advocates describe both methods as "frictionless" solutions that reduce human error and fraud, these systems introduce new risks.

Literature contrasts the intended security of biometric systems with their actual vulnerabilities. Biometric traits are depicted as robust barriers that prevent minors from circumventing age restrictions (Murray et al., 2025; Pasquale et al., 2020). However, both cybersecurity researchers and adolescents have demonstrated that these mechanisms can be easily bypassed. For example, verification systems may be spoofed using deepfakes, voice recordings, or even by presenting a printed photograph of an adult's face to a webcam (Murray et al., 2025; Pasquale et al., 2020; Woodley et al., 2025). As a result, achieving high accuracy requires specialized, invasive hardware, such as iris scanners, which are not widely accessible or practical for routine internet use (Pasquale et al., 2020).

The literature also emphasizes that both verification and estimation methods compromise user anonymity and contribute to the normalization of corporate surveillance. Although some proponents claim that age estimation is less intrusive than submitting identification-based verification, generating these estimates requires collecting behavioral data, such as GPS locations, IP addresses, cookies, and browsing history (Stardust et al., 2024; van der Hof & Ouburg, 2022). At the same time, biometric verification requires centralized databases containing permanent physiological traits. Australian adolescents have expressed significant concern that these databases are targets for hackers, increasing the risk of extortion and exposure of irreparable personal data (Woodley et al., 2025). Privacy advocates argue that the widespread adoption of either system conditions users to accept corporate monitoring as a prerequisite for digital participation (Livingstone et al., 2024; Stardust et al., 2024).

Researchers also highlight a significant legal paradox in both approaches: to protect children, biometric and AI systems must proactively profile and process sensitive data, often without verifiable parental consent. The processing of minors' special-category physiological or behavioral data directly violates privacy regulations, such as the GDPR and COPPA, which are intended to uphold age-verification laws (Murray et al., 2025; van der Hof & Ouburg, 2022). Additionally, because age estimation involves a margin of error, it does not provide the legal certainty required for strict regulatory compliance (van der Hof & Ouburg, 2022).

In summary, biometric age assurance substitutes the friction of traditional identifiers with continuous algorithmic surveillance. The academic debate focuses on whether the perceived need for online child protection justifies the normalization of invasive tracking. Analysis of the literature shows that the claimed protective benefits of these systems are outweighed by fundamental limitations, including systemic bias, exploitable vulnerabilities, and persistent privacy violations. The value of biometric age verification and estimation should be evaluated not by technological innovation alone, but by weighing their efficacy against the harm they impose on privacy and anonymity.

Attribute-Based Verification

Attribute-based verification enables users to confirm explicit eligibility requirements without revealing unnecessary personal information, such as names, addresses, or identification numbers (Murray et al., 2025). In contrast to identification-based or biometric methods, attribute-based systems authenticate user attributes to grant access. This method has proved to be a promising technological solution for organizations seeking to reconcile legal regulations with digital privacy protection. Figure 1 below shows how each verification method contrasts in its privacy and assurance capabilities.

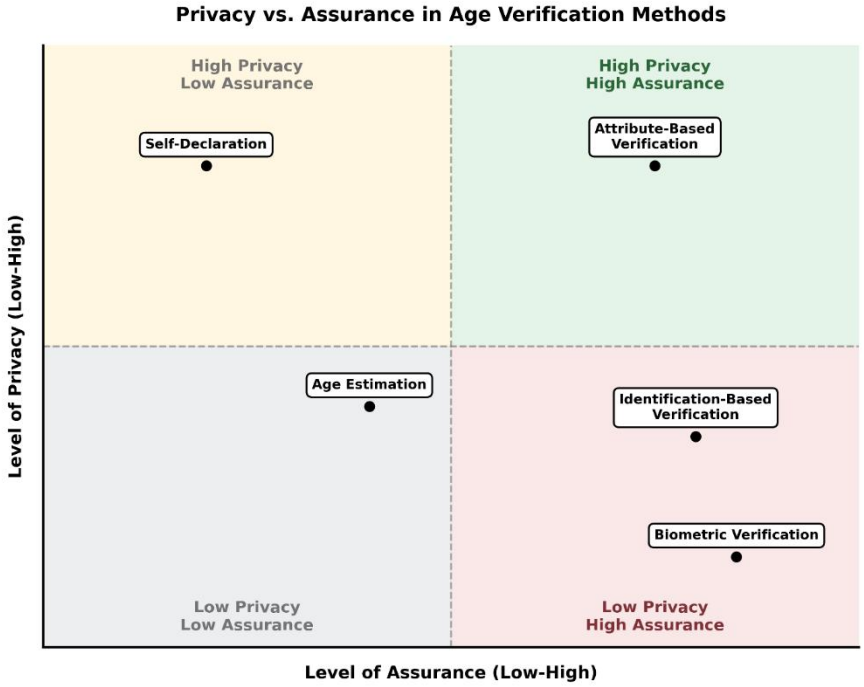

Figure 1. This figure illustrates the primary trade-off identified in the literature between digital anonymity and regulatory gatekeeping. Traditional methods force a compromise between high privacy and high assurance. Attribute-based verification is positioned in the upper-right quadrant as the current theoretical ideal.

Van der Hof and Ouburg (2022) and Murray et al. (2025) advocate for attribute-based systems as the most effective approach to age verification, presenting them as a practical realization of "privacy by design." Utilizing Privacy Enhancing Technologies (PETs), such as cryptographic age tokens, these decentralized systems authenticate an individual's age group directly on their personal device, thereby avoiding the transmission of sensitive personal data to a central server (Murray et al., 2025; Van der Hof

& Ouburg, 2022). Murray et al. (2025) identify open-source tools such as Yivi (formerly IRMA) as exemplary, emphasizing their ability to verify a user's age without revealing their precise identity. By removing centralized repositories of personal data, proponents contend that attribute-based verification reduces the risks of data breaches, data monetization, and identity theft associated with other methods (Murray et al., 2025).

However, user perspectives reveal a significant gap between the theoretical privacy protections of attribute-based verification and end-users' perceptions. While legal and cybersecurity scholars frequently present digital tokens as decentralized safeguards against surveillance, studies suggest that users do not share this optimism. For instance, Woodley et al. (2025) found, in a qualitative study of Australian adolescents, that many view "temporary" digital tokens and digital IDs with suspicion, expressing concerns that these mechanisms facilitate the centralization of personal data and monitoring of their activities. Participants even compared digital tokens to "vaccine passports," associating them with possible government or corporate censorship. This notable contradiction between scholarly intent and user distrust underscores the importance of the user perspective in analyses of attribute-based verification. For future research, studies should investigate the drivers of user distrust and assess which strategies most effectively bridge the privacy literacy gap.

From an efficacy standpoint, the literature identifies practical barriers to the adoption of attribute-based systems. Livingstone et al. (2024) caution that genuinely decentralized token systems are not widely available or implemented in the consumer market. Furthermore, Murray et al. (2025) observe that these systems shift security responsibility to individuals, introducing localized vulnerabilities, such as device theft or social engineering, that could compromise the security of passcode-protected verification applications on users' devices. Crepax et al. (2022) further note that child-specific PETs remain to be developed, as most controls are not designed to address minors' evolving capacities and vulnerabilities.

In summary, recent scholarship demonstrates that attribute-based verification offers the most balanced technological approach to meeting legal requirements while preserving privacy. However, despite these theoretical strengths, attribute-based systems face critical limitations in real-world

applications. Specifically, challenges in market availability, device-level security, and user trust constrain their effectiveness in protecting privacy and anonymity. Furthermore, technical features alone are inadequate, as user skepticism remains a significant barrier to adoption.

Conclusion

The legislative push for age verification (AV) to protect minors online has created a crisis for digital privacy and anonymity. While lawmakers advocate high-assurance methods, existing literature shows that relying on technology alone introduces significant new vulnerabilities. Moving away from self-declaration causes the collection of sensitive personally identifiable information (PII) and physiological data. Consequently, AV systems force society to confront a trade-off: efforts to protect youth expose both children and adults to data breaches, algorithmic biases, and persistent corporate surveillance.

These privacy compromises are exacerbated by flaws in many high-assurance systems that are easily circumvented by youth. Among the alternatives, attribute-based verification currently represents the most promising compromise. This approach theoretically reduces the risks of surveillance and identity theft associated with centralized databases. Nevertheless, despite their security, the adoption of attribute-based systems remains limited due to market availability and user distrust.

Given the disconnect between privacy protections and public perception identified throughout this literature review, future research should prioritize building user trust and addressing the privacy literacy gap. This directly addresses documented user skepticism and suspicion toward privacy-preserving technologies, especially among youth who may perceive digital tokens as surveillance tools. Thus, efforts to design transparent, user-centered, decentralized systems must account for user concerns. Additionally, future research should empirically evaluate specific educational strategies that clarify and demonstrate the privacy-preserving features of attribute-based tokens to both youth and adults.

References

Abdulla, S. M. (2025). (2025). “I shouldn’t have to scan my face to play a video game”: Dissonance in harm and values in children’s online media policy. Paper presented at the 271–287. https://doi.org/10.1145/3757887.3763015

Angel, M. '. i. P., & Boyd, D. (2024). (2024). Techno-legal solutionism: Regulating children's online safety in the united states. Paper presented at the *Proceedings of the 2024 Symposium on Computer Science and Law,* Boston, MA, USA. 86–97. https://doi.org/10.1145/3614407.3643705 https://doi.org/10.1145/3614407.3643705

Bowler, L. J. (2026). The digital rights of children and youth: An annual review of information science and technology (ARIST) paper. *Journal of the Association for Information Science and Technology,* https://doi.org/10.1002/asi.70048

Crepax, T., Muntés-Mulero, V., Martinez, J., & Ruiz, A. (2022). Information technologies exposing children to privacy risks: Domains and children-specific technical controls. *Computer Standards and Interfaces, 82* https://doi.org/10.1016/j.csi.2022.103624

Henderson, E. M., Law, E. F., Palermo, T. M., & Eccleston, C. (2012). Case study: Ethical guidance for pediatric e-health research using examples from pain research with adolescents.*37*(10), 1116–1126. https://doi.org/10.1093/jpepsy/jss085

Hokke, S., Hackworth, N. J., Quin, N., Bennetts, S. K., Win, H. Y., Nicholson, J. M., Zion, L., Lucke, J., Keyzer, P., & Crawford, S. B. (2018). Ethical issues in using the internet to engage participants in family and child research: A scoping review. *PLoS ONE, 13*(9) https://doi.org/10.1371/journal.pone.0204572

Jarvie, C., & Renaud, K. (2024). Online age verification: Government legislation, supplier responsibilization, and public perceptions. *Children, 11*(9) https://doi.org/10.3390/children11091068

Livingstone, S., Nair, A., Stoilova, M., Hof, S., & Caglar, C. (2024). Children's rights and online age assurance systems the way forward. *International Journal of Children's Rights, 32*(3), 721–747. https://doi.org/10.1163/15718182-32030001

Murray, A., Chhipa, H., & Yerby, J. (2025). Cyber risk, privacy, and the legal complexities of age verification for adult content platforms. *Issues in Information Systems, 26*(4), 332–347. https://doi.org/10.48009/4_iis_2025_127

Pasquale, L., Zippo, P., Curley, C., O'Neill, B., & Mongiello, M. (2022). Digital age of consent and age verification: Can they protect children? *IEEE Software, 39*(3), 50–57. https://doi.org/10.1109/MS.2020.3044872

Stardust, Z., Obeid, A., McKee, A., & Angus, D. (2024). Mandatory age verification for pornography access: Why it can't and won't 'save the children'. *Big Data and Society, 11*(2) https://doi.org/10.1177/20539517241252129

Turvey, J., McKay, D., Kaur, S. T., Castree, N., Chang, S., & Lim, M. S. C. (2024). Exploring the feasibility and acceptability of technological interventions to prevent adolescents' exposure to online pornography: Qualitative research. *JMIR Pediatrics and Parenting, 7* https://doi.org/10.2196/58684

van der Hof, S., & Ouburg, S. (2022). 'We take your word for it' — A review of methods of age verification and parental consent in digital services. *European Data Protection Law Review, 8*(1), 61–72. https://doi.org/10.21552/edpl/2022/1/10

Woodley, G., See, H. W., O'Neill, B., Green, L., Staksrud, E., & Haskell-Dowland, P. (2025). Australian teen voices on age verification and age assurance measures. *Policy & Internet, 17*(4), e70019. https://doi.org/10.1002/poi3.70019

Yar, M. (2020). Protecting children from internet pornography? A critical assessment of statutory age verification and its enforcement in the UK. *Policing, 43*(1), 183–197. https://doi.org/10.1108/PIJPSM-07-2019-0108