Issues in Information Systems
Volume 26, Issue 4, pp. 332-347, 2025

DOI: https://doi.org/10.48009/4_iis_2025_127

Cyber risk, privacy, and the legal complexities of age verification for adult content platforms

Alana Murray, Mercer University, *alana.francespearle.murray@live.mercer.edu*
Huma Chhipa, Mercer University, *huma.s.chhipa@live.mercer.edu*
Johnathan Yerby, Mercer University, *yerby_jm@mercer.edu*

Abstract

Since 2023, laws mandating age verification for online adult content have introduced serious cybersecurity and privacy challenges. While these laws aim to protect minors, they often compel platforms to collect sensitive user data, increasing risks of identity theft, data breaches, and surveillance. In response, companies like Pornhub have withdrawn from certain U.S. states, prompting users to turn to VPNs and other potentially insecure access methods. This paper explores the intersection of regulatory compliance, cybersecurity, and digital privacy in the context of mandatory age verification systems. It analyzes risks stemming from third-party verification vendors, inconsistent data retention policies, and technical vulnerabilities in identity-based authentication. Using a comparative framework, the study evaluates three common verification approaches: identification-based, biometric, and attribute-based, assessing their relative strengths, weaknesses, and legal implications. Attribute-based verification emerges as the most privacy-preserving and cybersecurity-conscious option. The paper offers policy and technical recommendations to help platforms meet compliance obligations while minimizing harm. These findings aim to inform legislators, platform providers, and cybersecurity professionals seeking effective and responsible verification strategies in an evolving digital landscape.

Keywords: age verification, digital identity, biometric authentication, attribute-based access control, privacy regulation, adult content compliance

Introduction

The proliferation of online adult content has prompted new legislation to prevent minors from accessing sexually explicit material. In January 2023, Louisiana enacted Act 440, which mandates age verification for websites containing a substantial proportion of adult content (Louisiana State Legislature, 2022). This legislative initiative marked a broader trend of mandating age verification for adult content online. In response, major adult content platforms such as Pornhub and its parent company Aylo, have ceased operations in several states, citing serious concerns over user privacy, data security, and legal liability (Free Speech Coalition, 2025; Gonzalez, 2024). While Aylo enforces rigorous identity verification for content creators, extending the same standards to its estimated five billion monthly visitors presents a far greater cybersecurity and operational challenge (Semrush, n.d.).

While much of the legal debate has focused on First Amendment implications, an equally pressing but less explored issue is how companies can implement these regulations without sacrificing security and privacy.

Age verification requirements introduce a complex and evolving cyber risk landscape not only for adult content providers, but also for users who are asked to submit personally identifiable information (PII), such as government-issued IDs or biometric data. Absent proper safeguards, such data becomes a high-value target for cybercriminals. The adult content industry faces significant obstacles to securely implementing verification. Compounding the issue, many state laws include vague or insufficient guidance regarding data storage, retention, disposal, and breach notification, leaving open significant questions about who is responsible for protecting this sensitive information.

This paper explores the practical, legal, and technical challenges posed by mandatory age verification laws in the United States. It highlights the cybersecurity risks that stem from data collection, third-party vendor reliance, and the inadequacy of many existing verification methods. It analyzes security-related liabilities, vendor vulnerabilities, and the weaknesses of current verification systems. Additionally, the paper evaluates emerging approaches to age verification: identification-based, biometric, and attribute-based verification. Lastly, it proposes policy recommendations to prioritize user privacy while meeting regulatory obligations.

Legal Literature Review

Age verification

Online age verification has become increasingly common across industries, driven by regulatory pressures and social concerns. From online gambling and alcohol sales to gaming and social media platforms, companies are implementing mechanisms to ensure age-appropriate access to digital services. YouTube, TikTok, and Instagram have introduced age-gating and content filtering features to comply with child safety regulations and advertising standards (Marsden, 2023). These developments reflect a broader societal expectation that digital environments mirror offline age-related restrictions.

In this context, lawmakers have applied the logic of age verification to adult content access, primarily as a tool for child protection. By requiring users to prove they are legally adults, legislators seek to reduce the exposure of minors to sexually explicit material. This rationale aligns with long-standing restrictions on youth access to regulated goods and services such as alcohol, gambling, and firearms (Van der Maelen, 2019). Yet, unlike face-to-face transactions, online environments pose distinct challenges—particularly regarding impersonation, scalability, and enforcement. Research suggests the average age of first exposure to pornography is approximately thirteen, further reinforcing the urgency policymakers feel in restricting youth access to adult content (Marsden, 2023).

The U.S. has grappled with this issue of online safety for decades. The 1996 Communications Decency Act (CDA) represented one of the earliest federal attempts to regulate online access to pornography, including provisions that criminalized the transmission of "indecent" content to minors. However, the Supreme Court struck down much of the CDA in Reno v. ACLU (1997), ruling that its language was overly broad and vague and thus violated the First Amendment. In response, legislators pursued narrower pathways, such as the Children's Online Privacy Protection Act (COPPA) of 1998, which focused on limiting the collection of personal information from children under thirteen rather than restricting access to adult content.

More recently, increased internet accessibility among minors, and growing concerns over the psychological impact of early exposure to explicit content have reignited efforts to implement age verification. At the state level, several legislatures have introduced or passed laws compelling commercial entities that host adult content to verify users' ages before granting access (Free Speech Coalition, 2025). While intended to protect children, these laws raise substantial questions about privacy, cybersecurity, and the technological feasibility of compliance across diverse platforms.

Relevant laws

As of June 2025, 18 states have passed an age verification law for adult content, with six scheduled to be enacted within the year and sixteen being introduced into state legislatures, including District of Columbia (Free Speech Coalition, 2025). While the precise language of these laws varies, they typically require commercial entities that host adult material to implement "reasonable" age verification measures. Measures include government-issued ID submissions, biometric scans, or third-party verification services. The legal rationale behind these regulations is primarily grounded in child protection, mirroring existing restrictions on age-restricted activities such as gambling and alcohol consumption. However, these statutes also raise significant concerns about their effectiveness, enforceability, and implications for privacy and cybersecurity (Mounica, 2024).

One of the most widely referenced legislative models is Louisiana's Pornography Age Verification Enforcement (PAVE) Act of 2023, which mandates that websites containing a substantial amount of adult content must verify users' ages before granting access (Brown, 2024). Other states, including Texas, Utah, and Virginia, have enacted similar laws, each with slightly different definitions of what constitutes a "commercial entity" and "substantial amounts" of indecent content. For example, while Louisiana's PAVE Act targets websites with more than 33.3% adult content, Kansas's SB 394 sets the threshold at 25%. These variations affect whether mixed-content platforms like Reddit or adult-centric services like OnlyFans fall under state jurisdiction. The lack of uniformity in definitions and enforcement across state lines complicates compliance for multi-jurisdictional platforms (Holmes, 2023; Yerby & Vaughn, 2022).

Adult industry advocacy group, the Free Speech Coalition, is a major lobbying arm for adult content creators and consumers. Along with tracking age verification bills nationwide, the Coalition has sued multiple states attempting to enact verification laws. Their suit against Texas Attorney General Ken Paxton's enforcement of HB 1181 escalated to the Supreme Court of the United States. In 2025, The Court voted in favor of Paxton, allowing age verification usage in the state, framing the required verification practices as an 'incidental burden' (Free Speech Coalition, Inc. v. Paxton, 606 U.S. __ 2025).

One recent and noteworthy example of evolving state legislation is Georgia's *Protecting Georgia's Children on Social Media Act* (SB 351), signed into law in 2024 and scheduled to take effect in July 2025. Although framed primarily as a social media regulation, the law includes broad provisions that extend well beyond traditional platforms. It mandates age verification for access to any "material that is harmful to minors," including content that, by "contemporary community standards," is considered to "pander to prurient interests." This vague and expansive phrasing echoes terminology from obscenity law and could encompass a wide array of digital content, not just pornography, but also medically accurate sexual education materials and expressive content aimed at older teens (Legoas, 2025).

Georgia's law requires social media providers to make "commercially reasonable efforts" to verify the age of users (Georgia General Assembly, 2024). According to the statute (Senate Bill 351 and Ga. Code Ann. § 39-6-2), these efforts may include submitting a signed form via fax, email, or mail; guardian confirmation through phone or video call; providing a parent's government-issued ID or payment card; or obtaining parental consent via email. The law also permits "any other commercially reasonable method" (Georgia General Assembly, 2024).

By embedding age-gating provisions within a law that also regulates school curricula and minors' access to social media, Georgia's approach reflects a broader trend of combining child safety measures with cultural or moral enforcement. Critics argue that this legal ambiguity invites overreach, risking the misclassification of legitimate educational or artistic content as "harmful," and raising serious First Amendment and privacy concerns (Legoas, 2025).

In June 2025, just days before SB 351 was set to take effect, U.S. District Judge Amy Totenberg issued a preliminary injunction blocking its enforcement, citing violations of free speech protections. This ruling is consistent with similar decisions in at least seven other states where courts have temporarily blocked comparable laws on constitutional grounds (Totenberg, 2025). Despite the injunction, some adult content platforms have already implemented access restrictions for Georgia users. The ruling highlights growing judicial skepticism about whether such laws are sufficiently narrow to justify their intrusion on protected expression. At the same time, the fragmented legal landscape, especially the divergence between lower court rulings and Supreme Court precedent, places adult content providers in increasingly uncertain legal positions.

Legal challenges have also emerged over potential constitutional conflicts. Critics argue that mandatory age verification restricts lawful access to protected content, thus violating the First Amendment (Holmes, 2023). Others raise privacy concerns, particularly around the collection and storage of personally identifiable information (PII). Section 230 of the Communications Decency Act, which shields platforms from liability for user-generated content, could be eroded if age verification laws force companies into active gatekeeping roles. Some legal experts have warned that these mandates may deter users from accessing adult content entirely, raising concerns over state overreach (Eidelman & LaFrance, 2025).

U.S. District Judge Timothy Brooks ruled that Arkansas Act 689, The Social Media Safety Act, would violate the First Amendment "because it is facially content-based restriction on speech that is not narrowly tailored to serve a compelling government interest" (Buckner, 2025). The judge further ruled that it would also violate the Plaintiff's Fourteenth Amendment right to due process because of the vagueness.

Beyond these constitutional debates, practical ambiguities abound. Many state laws do not specify clear standards for how long verification data can be retained, whether it may be monetized before deletion, or what safeguards must be in place. Critics argue that temporary data retention for profit undermines user privacy and creates vulnerabilities for exploitation. If third-party verification vendors store data longer than permitted or mismanage it altogether, companies relying on those services may still be held responsible. These practices illustrate an "ask for forgiveness, not permission" approach, where compliance with the letter of the law supersedes long-term data security planning (Dorner, 2023).

The rise of third-party age verification vendors has also created a lucrative but underregulated industry. Some vendors operate with minimal cybersecurity transparency, yet they are now empowered to collect sensitive identification data under the guise of legal compliance (Scheffler, 2024). Critics warn that these systems could become targets for cybercriminals or serve as vectors for blackmail, especially given the social stigma surrounding adult content consumption (Weissmann, 2024). Most age verification laws fail to mandate encryption standards, require breach notifications, or enforce stringent data minimization. A few states, such as North Dakota, unsuccessfully attempted to explore less invasive alternatives like device-based verification, which authenticate users without collecting PII (Boden, 2025). However, the scalability and legality of such approaches remain debated.

At the federal level, the proposed Shielding Children's Retinas from Egregious Exposure on the Net (SCREEN) Act would require platforms to use more sophisticated verification systems and impose steep penalties for noncompliance. While its intent is to standardize best practices for protecting minors, critics argue it may inadvertently punish smaller platforms or create disproportionate compliance burdens due to technological constraints.

Age verification laws are not exclusive to American legislatures; the United Kingdom has pursued similar measures since 2019. The UK's Online Safety Act (2023), effective July 2025, mandates age verification

for pornography and harmful content, including suicide, bullying, and violence (Department for Science, Innovation and Technology, 2024). In France, Aylo temporarily halted operations due to age verification laws, resuming access after the Administrative Court of Paris suspended enforcement (Hartmann, 2025).

Historically, the European Union (EU) lacked a definitive age verification requirement for adult content, and what counts as a 'risk' for minors. However, under the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA), digital content providers were frequently obligated to verify age to ensure parental consent for social media. In recent years, multiple member countries sought to clarify when verification was needed and through what mediums. By 2026, EU Member States anticipate adopting eIDAS, or national digital identities, potentially incorporating a 'mini wallet' for digital age verification (Windwehr and Hancock, 2025a). Both EU and non-EU countries are facing similar arguments opposing age verification laws, citing logistical and privacy obstacles.

Though these laws aim to shield minors from premature exposure to adult content, their real-world efficacy remains in question. The unclear legal boundaries, uneven enforcement, and potential for data abuse all signal the need for a more nuanced and harmonized legal framework (Yerby & Vaughn, 2022). Platforms like OnlyFans and Reddit, which occupy separate roles in the adult content ecosystem, may require distinct legal treatment. As it stands, there are legitimate concerns that these laws may inadvertently create new forms of vulnerability and exploitation—for minors and adults alike.

Cybersecurity Risk Landscape

According to Strupczewski (2021), cyber risk is defined as an operational threat arising from the performance of digital activities that can jeopardize information assets, ICT resources, or organizational infrastructure. Strupczewski's definition identifies three key components of cyber risk: (1) the source of the threat, including cyberwarfare, human error, or natural disasters; (2) the objects at risk, such as data, infrastructure, or digital assets; and (3) the potential impacts, including operational disruption, reputational damage, or civil liability. These risks may originate from malicious external actors, insider threats, or technological flaws. Cyber risk management asks organizations to address three critical questions: Where does the threat originate? What assets are at risk? And what are the potential tangible and intangible impacts of a breach? In the context of age verification, these include attacks on API-based verification systems, cross-site scripting (XSS), phishing attempts that spoof verification platforms, or exploitation of weak links in the data supply chain.

Mandated age verification systems create a significant cybersecurity risk landscape for both users and service providers. At the core of these systems is the collection and processing of highly sensitive data, such as driver's licenses, credit card numbers, or biometric information, which can easily become targets for cybercriminals. The use of third-party vendors for verification compounds this risk, particularly when those vendors lack sufficient transparency or adherence to robust cybersecurity frameworks. In several known cases, vendors have relied on outdated encryption protocols or retained user data longer than permissible, creating unnecessary exposure.

Cyber Risk Applications in Practice

When examining how cyber risk theory applies to adult content platforms, several practical dimensions emerge, especially concerning risk sources, exposed objects, and potential impacts. According to NIST SP 800-30, cyber risks may stem from human error, structural failures, natural disasters, or deliberate attacks. For adult platforms, however, the most significant sources are malicious actors exploiting digital authentication systems, insider threats, and vulnerable third-party vendors. These risks are heightened under laws that classify both the platform and its verification provider as commercial entities, jointly responsible for compliance (Marsden, 2023).

Pornhub currently operates in Louisiana despite the PAVE legislation, as verification is handled through a digital driver's license platform called LA Wallet. Users are redirected from the site to its third-party verification partner, AllPassTrust, which then communicates with the LA Wallet system through an API. However, security researchers and privacy advocates have raised concerns that this model conditions users to share sensitive data with little scrutiny, opening the door to phishing attacks that impersonate legitimate verification portals (Eddy, 2023). Moreover, Louisiana's Office of Motor Vehicles was breached in 2023, compromising millions of driver's license records (Lyngaas, 2023). This illustrates how reliance on digital identity ecosystems can magnify risk.

AllPassTrust further complicates the picture. Despite serving as a gatekeeper for American users, it is based in Cyprus and has been shown to use unencrypted protocols and self-signed SSL certificates—both considered high-risk practices (Malatesta & Glover, 2016). If data is intercepted during the API handoff between LA Wallet and AllPassTrust, Pornhub could still be held liable, especially given the U.S. legal precedent that holds companies responsible for data breaches by their vendors (Evans, 2022). While Aylo can afford to develop or contract proprietary verification systems, smaller competitors face either steep third-party vendor costs or the strategic risk of noncompliance. Beyond vendors, the websites themselves may introduce vulnerabilities. Like mainstream platforms, adult content sites often rely on cookies and tracking scripts, making them targets for cross-site scripting (XSS), HTML injection, and other attacks (Sobrier, 2011).

Cyber Risk Objects and Impacts

The objects exposed include user accounts tied to names and credit cards, age verification databases, and backend servers processing authentication requests. Breaches could result in the exposure of explicit browsing activity linked to real-world identities, triggering reputational damage or blackmail risk. Financially, the stakes are just as high: As of 2025, at least eight U.S. states have implemented civil fines for noncompliance with age verification laws, and seventeen allow private lawsuits filed by guardians on behalf of minors. Texas's HB 1181 enables the Attorney General to fine companies up to $10,000 per day for violations and already fined XHamster and Chaturbate under the law (Paxton, 2024). Some sites may choose to ignore compliance altogether, especially smaller operators that lack the technical infrastructure to implement robust age verification. Adult content viewers attempting to avoid identification may seek obscure or overseas-hosted sites that use insecure HTTP protocols or evade regulatory scrutiny. Such a shift not only undermines the policy goal of protecting minors but also increases the likelihood that users are exposed to malvertising, malware, or dark web content (Vallina et al., 2019).

Reputational risk is another major factor. The public perception that adult content is harmful, particularly to minors, exacerbates the consequences of any breach or legal dispute. As Evans (2022) notes, loss of stakeholder trust—especially in stigmatized industries—can accelerate regulatory backlash and investor retreat. Adult content companies face amplified reputational fallout if their data handling missteps become public, compounding legal and operational risk.

The 2015 data breach of Ashley Madison, a dating website marketed for extramarital affairs, exposed the personal information of over thirty-six million users. The fallout included reports of blackmail, job loss, divorce, and at least two suspected suicides (Lamont, 2016; Sharp, 2015). This incident illustrates the high stakes when companies that manage stigmatized or extremely sensitive user data fail to implement robust cybersecurity controls and maintain transparency. For adult content platforms, the reputational and legal risks of a breach can be similarly catastrophic.

If the insecure practices seen in the current age verification technologies are exploited, such vulnerabilities could lead to breaches that link users' identities with adult content access history. The reputational risk

could then be realized among users whose online activities are made public, inviting the dangers of the Ashley Madison leak to reemerge.

Vendor risk is amplified by unclear liability structures. If a third-party vendor fails to secure data or violates a state's data retention policy, the primary platform may still be held liable. These concerns are especially acute for companies like Pornhub or XHamster, which operate across multiple jurisdictions with differing legal standards. The convergence of sensitive data, inconsistent legal safeguards, and poorly regulated third-party providers creates a volatile cybersecurity environment. To mitigate these risks, age verification systems must prioritize secure architecture, data minimization, and robust vendor vetting. Without such controls, compliance efforts may paradoxically increase the very threats they seek to prevent.

Analysis of Solutions: Age Verification Technology Risk Assessments

Analyzing cyber risk management techniques demonstrates the importance of utilizing verification technologies that best mitigate cybersecurity threats while complying with state laws. The National Institute of Standards and Technology (NIST) offer organizations guidance on risk assessments through publications such as SP 800-30 ("Guide to Conducting Risk Assessments"), SP 800-37 ("Risk Management Framework"), and SP 800-53 ("Recommended Security Controls"). These frameworks help determine the degree and severity of harm associated with different verification technologies. The following analysis ranks three types of age verification methods by their cybersecurity risk profiles: identification-based, biometric, and attribute-based.

Identification-Based Verification

This method includes verifying age through government-issued IDs (e.g., driver's licenses, military IDs) or financial instruments (e.g., credit card data). Louisiana's LA Wallet is a prime example. Though only an adult-status attribute is shared, API connections introduce vulnerabilities, including brute force, scraping, and DDoS attacks (Salt Security, 2025). States lacking digital ID infrastructure often require users to upload scanned IDs or photos, requiring procedures far more invasive than traditional in-person checks. These methods may store full PII temporarily or longer, increasing exposure in the event of a breach. Moreover, identity-based verification has pushed some users toward VPNs or unsecured alternatives to avoid identification. VPN usage, however, introduces separate security concerns by shifting data exposure to potentially unregulated third parties (Vallina et al., 2019).

Having users of adult content websites get used to providing their identifications creates a sense of comfort and complacency where people fail to protect themselves. Disreputable adult sites may take advantage of the requirement and force visitors to turn over personal information that they later use for marketing, selling to data brokers, stolen by attackers, or even blackmail (Eddy, 2023). Scammers may also pose as verification services and get information directly sent to themselves. This model carries the highest risk due to the sensitivity of the data collected, the involvement of external vendors, and the complexity of securing API-based systems. The present researchers do not recommend it.

Biometric-Based Verification

Some age verification laws, like Virginia's SB 1515, permit biometric verification. Biometric methods use facial recognition to estimate user age, often through AI-driven analysis. Ondato, a leading provider in this space and a verification partner for OnlyFans, uses facial scanning technology to create a 3D biometric profile of the user's face. This system analyzes geometric features such as skin texture, facial proportions, and shape to generate an approximate age assessment. According to Ondato, their system also includes liveness detection to prevent spoofing with photographs, masks, or synthetic images, aiming to ensure that

a real human is present during verification (Ondato, 2025). Ondato claims to meet GDPR standards and offers solutions designed not to retain identifiable biometric data. However, the use of biometric technologies raises serious ethical concerns and potential regulatory compliance challenges, particularly when the subjects are minors. Notably, facial recognition may inadvertently process children's biometric data without parental consent, in violation of child protection norms (Van der Hof & Ouburg, 2022). Additionally, there is limited transparency regarding the storage, transmission, and deletion of biometric scans, and the transatlantic transfer of American user data to an EU-based processor introduces jurisdictional and legal complexity.

The NIST Face Analysis Technology Evaluation (FATE AEV) project evaluates the reliability of facial age estimation. In their child safety checks, the Mean Absolute Error (MAE), measuring the difference between one's estimated age and their true age, varies depending on the quality of the picture, race, and gender. Such algorithmic inaccuracies, especially in distinguishing 17-year-olds from 18-year-olds, could lead to legal liability for platforms that wrongly admit minors. Additionally, biometric submissions are vulnerable to spoofing via deepfakes or synthetic media. In states permitting citizens to file private civil suits against commercial entities, there is further cyber risk even if the third party accurately estimates a minor's age in most cases (Free Speech Coalition, 2025)

Though companies like Ondato may be GDPR-compliant, using EU-based vendors could expose American biometric data to foreign jurisdictions. Genetic and biometric data are often classified as sensitive personal information (SPI) under statutes such as California's CCPA (Thales Group, 2021), which introduce regulatory risk. Due to potential error rates, liability concerns, and data classification risks, biometric verification is not recommended as the primary compliance strategy.

Attribute-Based Verification

Attribute-based verification systems allow users to confirm essential eligibility information—such as being over the age of 18—without disclosing extraneous personal details like name, address, or ID numbers. One such solution is Yivi (formerly IRMA), developed by the Privacy by Design Foundation. This open-source tool enables users to authenticate specific attributes using a passcode-protected mobile app, where personal data remains stored locally on the user's device (Van der Maelen, 2019). This method prioritizes privacy and minimizes the risk of data exposure. Instead of transmitting full identification records, the platform simply verifies whether the user meets the required attribute (e.g., being over 18) using cryptographic proof. Attribute-based approaches have been endorsed by privacy advocates and supported by major tech platforms such as Meta and Pinterest, who argue that such systems meet legislative goals without compromising user data (Free Speech Coalition, 2025).

The adult content website can perform a cryptographic check to ensure the user attribute is authentic and the request is connected to a genuine device. Moreover, attribute-based authentication offers greater flexibility and interoperability across different platforms and services, as users can verify their age without relying on traditional forms of identification, meeting the needs of adult content viewing audiences and legislation. This not only enhances user privacy and security but also streamlines the age verification process, improving the user experience and reducing friction for users (York, 2023). Yivi's open-source code allows American companies to freely leverage the framework themselves, sidestepping foreign vendor concerns.

Beyond theoretical appeal, attribute-based verification is already in practice. ID.me, for instance, is a widely used system that enables users to verify attributes like military service, student status, or government employment for access to discounts and secure portals. The user can then authenticate to services like the

IRS or Social Security Administration without repeatedly re-entering sensitive details. ID.me is a provider that enables all three types of verification as shown in Table 1.

Table 1. Comparison of Digital Verification Methods

Category	Identification-Based Verification	Biometric Verification	Attribute-Based Verification
Example Use	Government-issued ID (driver license, passport)	Facial recognition, fingerprint scanning	Age verification ("Over 18"), student/military status
Verification Object	Personally Identifiable Information (PII)	Biometric Identifiers (SPI)	Self-declared or verifiable user attributes
Primary Risk Sources	API vulnerabilities, third-party vendors, database breaches, phishing, XSS	False positives, GDPR/CCPA compliance, biometric data breach, reputational risk	Social engineering, device compromise, physical security threats
Regulatory Implications	PII violations; civil lawsuits and regulatory penalties	SPI violations under laws like GDPR and CCPA	Lower legal exposure: risks depend on context or usage
Level of Data Sensitivity	High	Medium	Low to Medium
Authentication Methods	Secure API calls to back-end databases	Facial or fingerprint scanning, voice biometrics	Mobile app-based attribute, QR assertions, digital credentials
Representative Vendors	- LA Wallet - ID.me** - Yoti - Socure - IDnow - Shufti Pro - CLEAR - Jumio - Onfido - Mitek - AU10TIX - Socure - AllPassTrust	- Ondato - ID.me** - iProov - Yoti* - Veriff - NEC - Daon - FaceTec - Clearview AI	- Yivi - ID.me** - Trinsic - Yoti* - Dock.io - SpruceID - ZADA - Veres One - Evernym - Credential Commons

** Offers all three types of verification *Offers Biometric and Attribute

This model aligns closely with the principles of data minimization and user control. Because verification is processed locally, even in the event of a breach, centralized repositories of user identity data do not exist. However, risks such as device theft or social engineering remain. The Yivi solution, for instance, requires only a passcode to access the verification app, making it potentially vulnerable to social engineering attacks if the user's device is lost or compromised. In this instance, there is a single impacted device, a preferable outcome over a large database of PII being compromised.

Overall, attribute-based verification is considered the most secure and privacy-preserving approach to date. By verifying only what is necessary and storing data locally, it reduces the cyber threat exposures posed by other methods. As such, researchers recommend this approach as the most viable and responsible compliance solution for adult content platforms. Table 1 provides a comparison between the most common verification methods.

Recommendations for adult content platforms

Based on the legal, technical, and cybersecurity analysis presented in this study, several key recommendations emerge for both industry stakeholders and policymakers. These suggestions aim to strike a balance between protecting minors, respecting user privacy, and mitigating organizational risk.

Adopt attribute-based verification systems
Platforms should prioritize the implementation of attribute-based verification tools such as Yivi or similar privacy-preserving technologies. These systems verify only the necessary information (e.g., age) without exposing full personal identifiers, significantly reducing the potential for data breaches and identity theft. This method aligns with the principle of data minimization and is far less invasive than traditional ID or biometric-based approaches, which have proven controversial and risk-heavy. Endorsements from industry actors such as Meta and the Free Speech Coalition further reinforce their viability.

Apply data minimization principles
Consistent with best practices in cybersecurity and privacy law, companies should collect only the minimum amount of data necessary to complete verification. Overcollection not only increases the impact of a potential breach but also raises compliance burdens under laws like the GDPR and CCPA. Avoiding unnecessary collections such as biometric scans or full ID images reduces regulatory risk and makes systems more defensible during audits or litigation.

Vet and monitor third-party vendors
Adult content platforms often outsource age verification to outside technology partners, which can introduce significant third party and legal vulnerabilities. Companies must conduct thorough due diligence to ensure vendors comply with international standards (e.g., ISO 27001, SOC 2, GDPR, CCPA), maintain transparency about their data handling practices, and undergo regular independent audits. History has shown that vendor failures have led to major breaches and regulatory penalties in other industries, underscoring the need for accountability in this high-risk environment (Malatesta & Glover, 2016).

Implement cryptographic verification and secure APIs
Platforms should integrate cryptographic proofs (e.g., zero-knowledge attestations) and secure API architectures that validate a user's age without transmitting sensitive personal information. APIs should be protected against brute force, scraping, and injection attacks, and all data in transit should be encrypted. Implementing cryptographic methods not only reduces exposure but also enables platforms to maintain user anonymity while complying with the law.

Provide clear disclosures and opt-out mechanisms
Only 16% of adult content websites have assessable privacy policies (Vallina et al., 2019). Users should be informed in clear, accessible language, how their data is processed, who has access to it, and for how long it will be retained. Platforms should avoid legalese and include easy-to-understand privacy notices. Additionally, offering opt-out mechanisms or alternative verification methods (e.g., through attribute-based or local-device checks) can improve public trust, reduce friction, and mitigate backlash from privacy-conscious users.

Recommendations for policymakers

Standardizing regulatory requirements across jurisdictions
Currently, adult content providers must navigate a confusing patchwork of state-level laws with differing thresholds, definitions, and requirements. This legal fragmentation increases compliance costs, complicates enforcement, and may incentivize platform withdrawals from certain states (Yerby & Vaughn, 2022). A harmonized federal framework—or model legislation adopted across states—would create clarity and fairness while still protecting minors. This recommendation may be difficult to nationalize this type of program where each state may have drastically different preferences and tolerances.

Mandate cybersecurity controls and vendor accountability

Age verification laws must go beyond access restrictions and require specific technical safeguards. Mandating compliance with recognized security standards (e.g., NIST 800-53, ISO 27001) ensures a baseline level of protection. Legislators should also impose liability on vendors who mishandle data, including breach notification mandates, financial penalties, and explicit contractual accountability.

Encourage or endorse privacy-enhancing technologies
Many companies hesitate to adopt novel verification systems unless they are clearly permitted under law. Policymakers should take a proactive role by recognizing or certifying tools like Yivi, which provide age verification without collecting PII. This would create legal clarity, spur innovation, and signal that privacy-preserving compliance is not only acceptable but preferred. As legislation is enacted, the mechanisms of protection should be considered along with the requirements. Passing requirements without standards or mechanisms will create more problems, confusion, and cybersecurity risks.

Fund independent audits and technical evaluations
Lawmakers and regulatory agencies should fund or commission independent reviews of age verification technologies, particularly those involving AI and biometrics. Evaluations should assess algorithmic bias, false positive rates, accuracy in identifying minors, and data security risks. Without such oversight, the public is left to rely on vendor marketing rather than objective evidence.

Include explicit provisions on data retention and disposal
Too many current laws fail to specify how long verification data may be retained, whether it can be monetized, or how it must be disposed of. Policymakers must close these loopholes by requiring prompt deletion of data after verification, prohibiting resale or profiling, and mandating secure, auditable disposal protocols. These measures are critical to prevent future misuse and reduce long-term privacy risk.

Conclusion

The rapid expansion of age verification laws in the United States reflects a growing effort to shield minors from online adult content. While the intent of these regulations is legitimate, their implementation often introduces significant cybersecurity and privacy risks for both users and platforms. This paper has examined the legal landscape, the vulnerabilities associated with current verification technologies, and the emerging best practices that can mitigate those risks. Identification-based and biometric systems, while widely proposed, pose substantial concerns: ranging from data breaches and regulatory exposure to ethical dilemmas related to biometric surveillance and jurisdictional overreach. In contrast, attribute-based verification offers a path forward that upholds user privacy while enabling legal compliance. It reduces the attack surface by avoiding centralized storage of personal data and limits the potential for misuse or exploitation of sensitive information.

For adult content platforms, the strategic adoption of privacy-preserving verification methods like Yivi, combined with rigorous vendor management and secure implementation practices, offers a defensible and forward-compatible solution. For lawmakers, refining statutes to promote technical standards, vendor accountability, and user rights will improve both effectiveness and public trust.Age verification policy must move past binary questions of access and toward a more nuanced consideration of cybersecurity, user autonomy, and the long-term consequences of digital identity collection. If poorly implemented, these laws risk creating new forms of vulnerability in the name of protection. But with smart approaches, safeguarding both youth and privacy in the digital age is possible.

Call to Action
Policymakers must act now to establish meaningful safeguards for verification systems before widespread implementation further entrenches insecure or invasive practices. Industry leaders, researchers, and privacy advocates should collaborate to standardize secure, ethical, and scalable verification solutions.

Future Research
Future studies should assess how users respond to various age verification mechanisms, especially under state-mandated systems and explore the behavioral effects of deterrents such as VPN use or dark web migration. Further technical evaluations of emerging AI-based verification tools and their real-world error rates are also essential to inform regulatory decision-making.

References

Amy, J. (2025, June 27). *Judge blocks Georgia's social media age verification law, citing free speech concerns*. *Associated Press*. https://apnews.com/article/georgia-social-media-age-verification-law-lawsuit-51b4ce108f0d22adadc50d50e0392dd4

Act 440, 142, Louisiana State Legislature (2022).

Boden, A. (2025, February 20). Changes to North Dakota AV bill force FSC to withdraw support. Free Speech Coalition. https://www.freespeechcoalition.com/blog/north-dakota-av-bill-opposition

Brown, Ossie (2024, July 22). New Louisiana porn law. The Law Offices of Ossie Brown. https://ossiebrown.com/blog/louisiana-porn-law/

Buckner, M. (2025, April 1). *Federal judge blocks Arkansas social media age verification law*. *THV11*. https://www.thv11.com/article/news/politics/judge-arkansas-social-media-age-verification-unconstitutional/91-2ddb8f3a-008f-47bf-8721-860eed2c52d8

Dorner, U. (2023, July 12). *Ask permission, not forgiveness*. Forbes. https://www.forbes.com/councils/forbesbusinesscouncil/2023/07/12/ask-permission-not-forgiveness/

Eddy, M. (2023, January 4). *Louisiana's new porn law is a privacy time bomb*. *PCMag*. https://www.pcmag.com/opinions/louisianas-new-porn-law-is-a-privacy-time-bomb

Eidelman, V., & LaFrance, S.. (2025, January 14). Supreme Court may decide if the government can childproof the Internet. American Civil Liberties Union. https://www.aclu.org/news/privacy-technology/supreme-court-may-decide-if-the-government-can-childproof-the-internet

Evans, A. (2022). Enterprise cybersecurity in digital business: Building a cyber resilient organization. Routledge.

Face analysis technology evaluation (FATE) age estimation & verification. (n.d.). Retrieved April 2, 2025, from https://pages.nist.gov/frvt/html/frvt_age_estimation.html

Free Speech Coalition. (2025). *Age verification bills: Action center*. https://action.freespeechcoalition.com/age-verification-bills/

Georgia General Assembly. (2024). *Senate Bill 351: Protecting Georgia's Children on Social Media Act of 2024*. https://www.legis.ga.gov/legislation/66023

Georgia General Assembly. (2024). *Ga. Code Ann. § 39-6-2 (2024)*. https://www.legis.ga.gov/

Gonzalez, O. (2024, March 14). *Pornhub bans Texas*. *Gizmodo*. https://gizmodo.com/pornhub-pulls-out-of-texas-1851336939

Grimmelmann, J. (2024). The return of age verification laws. Communications of the ACM, 67(5), 34–36. https://doi.org/10.1145/3651865

Hendrickson, L. (2025, April 17). *What is age verification? Ensuring compliance and privacy online*. *Identity.com*. https://www.identity.com/what-is-age-verification/

Holmes, E. N. (2023, August 17). *Online age verification (Part II): Constitutional background* (CRS Legal Sidebar No. LSB11021). Congressional Research Service. https://crsreports.congress.gov/product/pdf/LSB/LSB11021

LA Wallet. (2024). Digital verification. *LA Wallet*. Retrieved February 24, 2025, from https://lawallet.com/digital-verification/#Verify-You

Lamont, T. (2016, February 27). *Life after the Ashley Madison affair*. *The Guardian*. https://www.theguardian.com/technology/2016/feb/27/what-happened-after-ashley-madison-was-hacked

Layng, K. (2009, October). Non-technical keys to keeping your personally identifiable information PII risk mitigation project on track. In *Proceedings of the 37th Annual ACM SIGUCCS Fall Conference: Communication and Collaboration* (pp. 223–228). ACM.

Legoas, M. (2025, January 7). *New Georgia law in 2025 will impact pornography websites: What is Senate Bill 351? The Augusta Chronicle*. https://www.augustachronicle.com/story/news/politics/state/2025/01/07/pornography-will-be-partially-blocked-under-new-georgia-law-what-to-know/77490065007/

Louisiana Division of Administration. (2025). *LA Wallet*. https://www.doa.la.gov/doa/ots/tech-spotlight/la-wallet/

Lyngaas, S. (2023, June 16). *Millions of Americans' personal data exposed in global hack*. CNN. https://www.cnn.com/2023/06/16/politics/cyberattack-us-government/

Malatesta, J. T. A., & Glover, S. S. (2016). A clear and present danger: mitigating the data security risk vendors pose to businesses. *Sedona Conference Journal* (Vol. 17, p. 761).

Marsden, C. (2023). Age verification laws in the era of digital privacy. *National Security Law Journal*, 10(2), 210-243

Mounica, S. (2024, September 23). Navigating the evolving landscape of age verification law in the US. Hyperverge.co. https://hyperverge.co/blog/age-verification-law/

Ondato. (2025). *AI-powered age verification*. Ondato. https://ondato.com/age-verification

Paxton, K. (2024, March 8). Attorney General Ken Paxton Wins After Pornography Companies Sued Texas Over Age Verification Requirements. https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-wins-after-pornography-companies-sued-texas-over-age-verification

Paxton, K. (2024, March 21). Attorney General Ken Paxton Sues Two More Pornog-ra-phy Com-pa-nies for Violating Texas Age Verification Law. https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-two-more-pornography-companies-violating-texas-age-verification-law

Privacy by Design Foundation. (2025). *What is IRMA?*. https://privacybydesign.foundation/irma-explanation/#topic

Reuters. (2021, September 30). Two people may have committed suicide after Ashley Madison hack-police. Reuters. https://www.reuters.com/article/business/two-people-may-have-committed-suicide-after-ashley-madison-hack-police-idUSL1N10Z12K/.

Salt Labs. (2025, February 26). *Salt Labs state of API security report Q1 2025* [PDF]. *Salt Security*. https://salt.security/api-security-trends

Sashchuk, D. (2024, October 30). *Age verification regulations in the United States of America*. *Veriff*. https://www.veriff.com/fraud/learn/age-verification-legalization-in-the-united-states-of-america

Scheffler, S. (2024). Age verification systems will be a personal identifiable information nightmare. Communications of the ACM, 67(7), 31–33. https://doi.org/10.1145/3660519.

Semrush. (n.d.). *Top trending adult websites globally*. *Semrush*. Retrieved July 14, 2025, from https://www.semrush.com/trending-websites/global/adult

Sharp, A. (2015, August 24). Two people may have committed suicide after Ashley Madison hack. *Reuters*. https://www.reuters.com/article/technology/two-people-may-have-committed-suicide-after-ashley-madison-hack-police-idUSKCN0QT1O6

Sobrier, J. (2011, April 28). Security flaws XSS, CSRF, SQL injection, HTML injection. Zscaler. https://www.zscaler.com/blogs/security-research/cross-site-scripting-xss-cross-site-request-forgery-csrf-sql-injection-html-injection-etc

Spangler, T. (2023, August 19). Pornhub parent company changes name to Aylo. *Variety*. https://variety.com/2023/digital/news/pornhub-parent-name-change-aylo-adult-entertainment-1235700312 .

Strupczewski, G. (2021). Defining cyber risk. Safety Science, 135, 105143. https://doi.org/10.1016/j.ssci.2020.105143

Tallahassee Democrat. (2025, January 3). Porn in Florida: As age verification takes effect, some sites ignore it, some block access. Tallahassee Democrat. https://www.tallahassee.com/story/news/politics/2025/01/03/some-porn-sites-blocked-but-others-ignore-florida-age-verification-law/77401109007/

Thales Group. (2021). *What is biometric data?*. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data

Totenberg, A. (2025, June 26). *Opinion & order granting preliminary injunction in NetChoice v. Carr (Georgia SB 351)*. U.S. District Court, Northern District of Georgia. Retrieved from NetChoice v. Carr Doc. 34.

U.S. Congress. (2025). *S.737 – Shielding Children's Retinas from Egregious Exposure on the Net (SCREEN) Act*. https://www.congress.gov/bill/117th-congress/senate-bill/737

Vallina, P., Feal, Á., Gamba, J., Vallina-Rodriguez, N., & Anta, A. F. (2019). Tales from the porn. Proceedings of the Internet Measurement Conference, 245–258. https://doi.org/10.1145/3355369.3355583.

Van Alstyne, M., Smith, M. D., & Lin, H. (2023). Improving Section 230, preserving democracy, and protecting free speech. Communications of the ACM, 66(4), 26–28. https://doi.org/10.1145/3584710

Van der Maelen, C. (2019). The Coming of Age of Technology. Delphi- Interdisciplinary Review of Emerging Technologies, 3

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

Weissmann, S. (2023, May 24). Age-verification legislation discourages data minimization, even when legislators don't intend that. R Street Institute. Retrieved April 17, 2024, from https://www.rstreet.org/commentary/age-verification-legislation-discourages-data-minimization-even-when-legislators-dont-intend-that/

Windwehr, S., & Hancock, S. (2025, April 29). *Age verification in the European Union: The Commission's age verification app*. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2025/04/age-verification-european-union-mini-id-wallet

Windwehr, S., & Hancock, S. (2025, April 23). *Digital identities and the future of age verification in Europe*. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2025/04/digital-identities-and-future-age-verification-europe

Yerby, J., & Vaughn, I. (2022). Deliberately confusing language in terms of service and privacy policy agreements. Issues in Information Systems, 23(2).

York, T. (2023). What's ABAC? How Attribute Based Access Control Works. Splunk. https://www.splunk.com/en_us/blog/learn/abac-attribute-based-access-control.html