Device-Based Age Assurance:
A Safer Approach to Ensuring Access to Age-Appropriate Content

Executive Summary

Age verification has become a priority for lawmakers in their efforts to make the internet a safer space. Unfortunately, current efforts to enact age verification laws to prevent minors from accessing adult content pose significant data privacy and security concerns, present Constitutional challenges to First Amendment free speech rights, increase barriers to proper platform compliance and enforcement by dissuading user retention, and can lead to negative outcomes from unintended user behavior. Age verification solutions must be properly implemented to achieve the primary goal of protecting children, while simultaneously preserving the privacy and Constitutional rights of adult consumers.

As such, there is a significant need for legislation that places the age assurance mandate at the source, on the device, to resolve these challenges. Device-based technology as a method of age assurance is technically feasible to implement and relies on elements that are already a common practice across industries. Device-based age assurance verifies a user's age through their device's operating system and shares the user's verified age or age range with the application, service, or website the user is attempting to reach, creating a safer, privacy preserving approach to age verification, while also addressing the various Constitutional and compliance challenges posed by existing iterations of current legislation.

Implications of Current Online Age Verification Laws

The current age verification requirements under recent legislation are ineffective and pose significant implications to the privacy and Constitutional rights of adults. In June 2022, Louisiana passed an age verification law requiring platforms and websites that contain "a substantial amount of adult material" to implement an age verification method prior to granting users access to the website's content. Since then, eighteen (18) additional states have followed suit. Requirements vary largely across states for what constitutes a reasonable age verification method, ranging from highly invasive methods such as uploading a government-issued identification (ID) card, to vague methods so long as they are "commercially reasonable."

While these age verification laws may be well-intentioned in protecting minors from accessing age-inappropriate content, they fail to do so. Additionally, they aim to subject adult users to upload personal information and sensitive data prior to accessing content, posing adverse consequences to user privacy and constitutionally protected speech. As current legislation

requires verification to occur on a per platform basis, adult users are required to upload or provide personal information numerous times across multiple platforms, significantly increasing the risk of misuse and phishing, to their information being compromised in data breaches, and potential widespread identity theft. Additionally, existing age verification mandates burden adult users' access to Constitutionally protected speech. Existing age verification laws, including Texas' H.B.1181, are actively undergoing challenges in district and appellate courts as well as the Supreme Court for harming the speech rights of adults by creating a government mandated, restrictive barrier to access.

Though some companies with a genuine interest in protecting children and the privacy of adult users may comply with these regulations and take users' safety and privacy into account, many companies and sites may not have the resources or desire to comply in a comprehensive manner. This results in a patchwork approach to compliance with age verification laws – each of the potentially hundreds of thousands of platforms may have their own systems or third-party vendors with a high degree of variance on how securely they store information, how much due diligence they have for third-party vendors, and how strongly they or their third parties uphold data deletion policies.

Additionally, existing age verification laws dissuade compliance. Compliant sites that implement proper verification protocols have experienced a significant exodus of users since adult users that do not want to share personal information will seek out non-compliant sites, many of which are located outside the jurisdictions of the states. This has the effect of naturally redistributing users to non-compliant platforms and websites. Many smaller platforms and websites who are not compliant continue operating without effective processes to verify the age of users, or without proper safeguards in place to protect the personal information collected from users. In the end, the goal of protecting minors online falls woefully short.

What is Device-Based Age Assurance

The most effective, secure, and equitable solution for protecting all users, both minors and adults alike, is to implement a mechanism that verifies a user's age only once and at the point of access to the internet: on the device. The user's age or age range can be shared with the application, online service, or website they are attempting to reach. This approach, otherwise known as device-based age assurance, would require a user's age to be independently verified one time by the device's operating system, and would securely store the user's age locally on the individual device.

When a user attempts to access a website containing adult content, the user's operating system would then share a user's verification status with the applicable website through a

secure Application Programming Interface (API), which would provide the website with a response on whether the user meets the defined age thresholds to access the platform. This approach ensures a seamless experience between the user and the platform that user is trying to access, eliminating the need to upload personal information to a third-party verification system or to each adult content platform visited, removing the barriers to access Constitutionally protected speech.

Device-based age assurance is straightforward and effective. The technology already exists and standardizes the age verification process, reducing potential points of failure including privacy, Constitutional, and compliance concerns with existing age verification laws. The crux of the approach requires collaboration with operating system companies, such as Apple (iOS), Google (Android), and Microsoft (Windows), to leverage existing infrastructure and technology to deploy a secure method to validate and store a user's age, and create a secure API in which a user's age or age range can be shared with the adult website in an anonymized and secure manner.

Technical Feasibility of Device-Based Age Assurance

Current hardware and software systems are already beyond the maturity-level required to deploy a device-based age assurance solution. Apple, Inc., one of the leading operating systems and technology companies, can be examined as a case study to demonstrate the existing technological feasibility of device-based age assurance. More recently, Google has deployed age assurance functionality in the United Kingdom.

Secure data stored by device manufacturers and operating systems can be accessed through readily available, trusted, and developed APIs. An API is a set of protocols that allow software programs to communicate and access specific data points from other operating systems, applications, or services. This API integration provides websites with the functionality to request information, including age information, directly from the device's operating system without requiring the website to authenticate the personal information of the user. This allows platforms and websites to request and access data stored within the device without needing to directly interact with the backend architecture of the device's operating system.

As an example, Apple already maintains a Wallet API that is capable of the functionalities required for device-based age assurance. The Verify by Wallet is an example of an API that allows integrations that share verified, authenticated age information to approved third party applications. The data shared is limited only to the integration's use case, ensuring the privacy of the device user. This prevents device manufacturers from oversharing user data beyond the approved use case and allows websites to minimize the amount of data they collect. Though

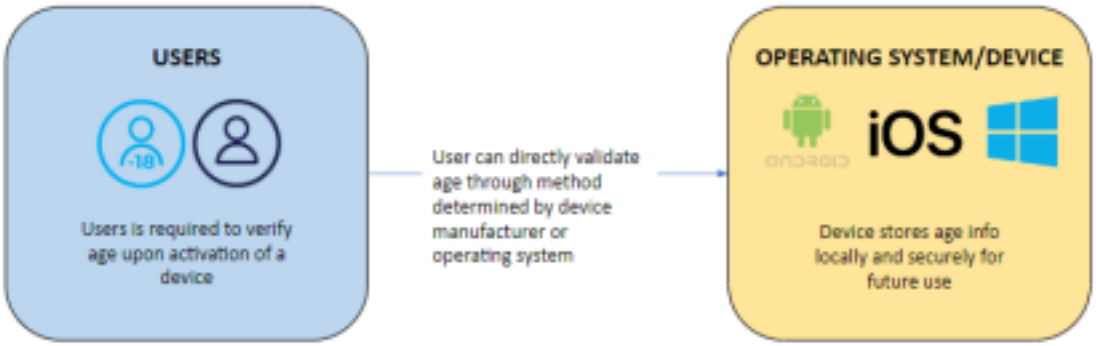
the method in which device manufacturers and operating systems may perform and collect age verification information can vary, the Verify by Wallet API demonstrates an example of the existing technology entities have in place to share limited personal data with third parties.

A Potential Implementation of Device-Based Age Assurance

By leveraging the above technology to securely store and share verified age information through APIs, it is possible to implement a highly effective device-based age assurance mechanism that addresses the unintended privacy risks of current, mandated platform-level age verification requirements. The user, device/operating system, and platforms/websites are all able to safely interact, verify ages using privacy-preserving approaches, and protect minors from accessing age-inappropriate content.

Step 1: Age Verification of the User

Upon activation of a device, a user will validate their age through commercially reasonable methods put into place by the operating system, such as inputting the required information on the local device.



Once the age information is verified, it can be stored locally on the device or by other secure methods implemented by the operating system. Storage on the device can be done so securely, similarly to how government-issued IDs are currently stored on devices.

Step 2: Websites Requiring Age Verification Must Implement Sufficient API Integrations

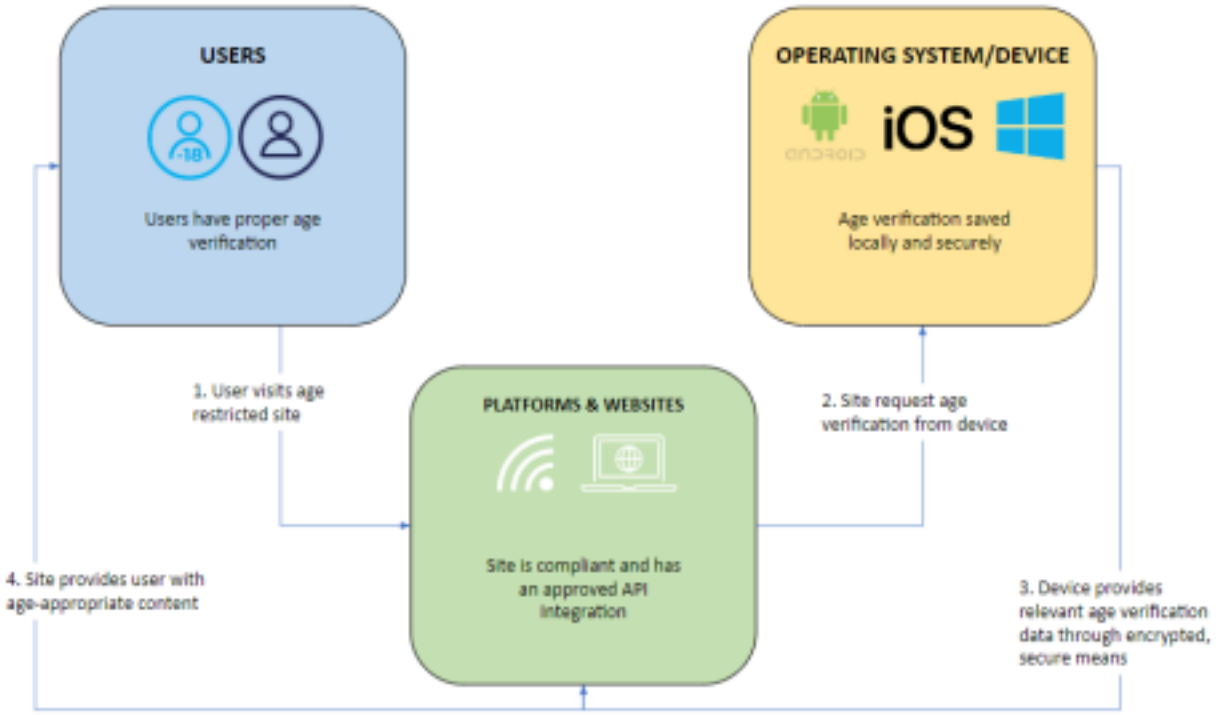
Any website that is legally required to verify the ages of their users must implement a sufficient API integration with operating systems. The API integration must be reviewed and approved by the operating system before the site can request and receive any age data.

APIs are a common practice and already exist on devices, major operating systems, websites, and applications. Websites and applications use APIs on a daily basis in order to communicate with other services without needing to access the other's codebase or backend architecture. Each API integration use case is tracked by the operating systems as standard procedure to ensure the traceability and accountability of websites using these APIs. Websites are required to provide full transparency into the identity information the app requests.

Step 3: User Attempts to Access Age Restricted Site

When a user attempts to visit a site using such an API, the site will send a request for the age verified data through the approved API. The API then receives and processes the request. Based on the agreed upon terms of the API integration, such as the use case for this information and the age data needed, the API will retrieve the necessary information from the operating system. The operating system could provide either the exact age of the user, or provide signals based on the legal thresholds (<13, <16, 18+, 18-) defined within the state. The device will then provide the verified age data to the site.

After obtaining age data, the site can then allow access or display permitted content to the user as per the site's age restriction policies. If a site is properly compliant, the user will not be able to access the site if the user's age is determined to be below the threshold to access.



Effective, Secure, and Equitable Age Assurance

Device-based age assurance is an effective, easy to implement, and technically feasible solution for preventing minors from accessing age-inappropriate material while protecting the privacy and Constitutional rights of adult users. By verifying a user's age through the device's operating system and securely sharing through an API to approved websites and platforms, device-based age assurance mitigates the inherent privacy risks, Constitutional challenges, and patchwork nature of compliance currently posed by existing age verification laws. In addition, a device based age assurance mechanism does not dissuade users from visiting compliant platforms and websites. Compliance with device-based age assurance would be considered better for business, reducing the number of non-compliant websites and therefore the opportunities for minors to access age-inappropriate content. Overall, the common goal of protecting minors online would be achieved.

Device-based age assurance is technically feasible to implement and can be securely leveraged across all platforms, apps, and websites. As demonstrated by Apple, one of the three major operating system companies, the innovations and technologies required to implement device based age assurance are already widely in use and could be easily updated to enable this assurance mechanism globally within a short time horizon. Users would only need to validate and share their personal information with their operating system, which many users already

trust with a high level of privacy and security. Device-based age assurance creates a simpler, more transparent and secure ecosystem for all parties, and fulfills its main purpose of protecting minors from accessing inappropriate content online.

///