FOSI
Family Online Safety Institute

Balancing Safety and Privacy: A Proportionate Age Assurance Approach

Visit Us
www.fosi.org

Email Us
fosi@fosi.org

Introduction

The era of widespread age assurance has arrived. Legislation and regulations are spreading around the world and companies are having to quickly adapt to multiple jurisdictions and rules - potentially contradictory in the case of age checks and user privacy, in their implementation. Before new laws are crafted at the state, federal or international levels, it is important that lawmakers understand and realize the degree to which age assurance options are already in place.

This paper attempts to illustrate the broad universe of companies, third party validators, government agencies and platforms that together have created a mosaic of solutions that balance the need to know a user's age (or age range) while preserving their privacy. It is critical that industry players continue to work together to both provide robust services and to plug any gaps.

It is also vital that governments actively engage the tech industry in ensuring that a comprehensive range of options, products and services are available to users while restraining from creating new, conflicting and onerous legislation with its own set of unintended consequences and complexity.

The moment we are in

Balancing online safety and privacy for children and teens has long been a challenge. Today, the tools and frameworks to make proportionate, privacy-preserving age assurance a reality appear to be within reach. Achieving that balance between safety and privacy has bedevilled policy makers and tech firms for decades, going back to the Child Online Protection Act or COPA Commission of 2000, which concluded that age verification technology was simply not there yet.

Fast forward twenty-five years, and we have seen both a maturation of the means to estimate or verify age as well as the onset of state, federal and international laws and regulations demanding that age assurance is in place. The recent implementation of the Online Safety Act in the UK has seen an impressive increase in the use of age assurance checks for adult sites, social media platforms and gambling apps. And standards bodies and government entities are establishing baseline requirements and conducting technology trials to better define effective, accurate age assurance processes.

What follows is our best effort to distill all that we have learned from our ongoing working group deliberations as well as our recent research and white paper. This is our general approach to age assurance including our philosophical underpinnings. What it is not is an attempt to craft model legislation at either the state or national level. Our hope is that FOSI members and the wider industry will take up this approach and thus negate the need for legislation that risks unintended consequences.

Core Principles

Any age assurance system should meet as many of the following foundational principles as possible:

✔ Is proportional to the risk, privacy-preserving, secure, interoperable, easy to use, high confidence and content neutral
✔ Adheres to local, national and international laws and regulations
✔ Is mindful of the free expression rights of users (including minors)
✔ Is effective without being intrusive
✔ Has considered national and international standards body recommendations
✔ Is flexible to emerging requirements

We believe that an age assurance solution should be proportional to the risks posed by the service or platform. In practice, this means that for the vast majority of websites, apps, and services that pose minimal risk to users, it is appropriate to use age assurance mechanisms with a lower level of confidence and invasiveness, if at all. For the minority of online activities that pose a high risk, it would be appropriate to require much greater levels of certainty and enhanced verification.

We believe that everyone has a role to play in making children's online experiences safer and age-appropriate. This includes governments, tech companies, parents, educators, child safety organizations, and the kids themselves. The tech industry has a specific part to play, from credential issuers and credential holders to operating systems, app store operators, apps and websites conducting age assurance and providing age appropriate experiences.

Age assurance is not an online safety solution in and of itself. Knowing the age or age range of someone is the first step - the real benefit comes from apps and platforms taking that information and providing age appropriate experiences to all users. By knowing the age or age range of their users, apps and platforms can deliver safer online experiences.

Legal and regulatory landscape

The US Supreme Court upheld a Texas law requiring age verification for adult websites. And while not currently required, the EU's Digital Services Act does require platforms to protect minors and implement appropriate measures to ensure their safety, which may include age verification depending on the platform's risk assessment.

At the federal level, the App Store Accountability Act would require app stores to verify users' age and to collect personal information of every user, regardless of age. This approach would prevent minors from accessing apps unless a parent approves. On the one hand, the Act would simplify the steps parents would need to take to limit their children's ability to download inappropriate apps and content. On the other hand, the Act doesn't cover the multitude of other sources of content beyond apps, including websites, platforms, games and more. The Act would also require the collection and storage of sensitive information *of all users* and would require the app stores to do this for apps that have no potentially harmful or inappropriate content in them, e.g., a weather app.

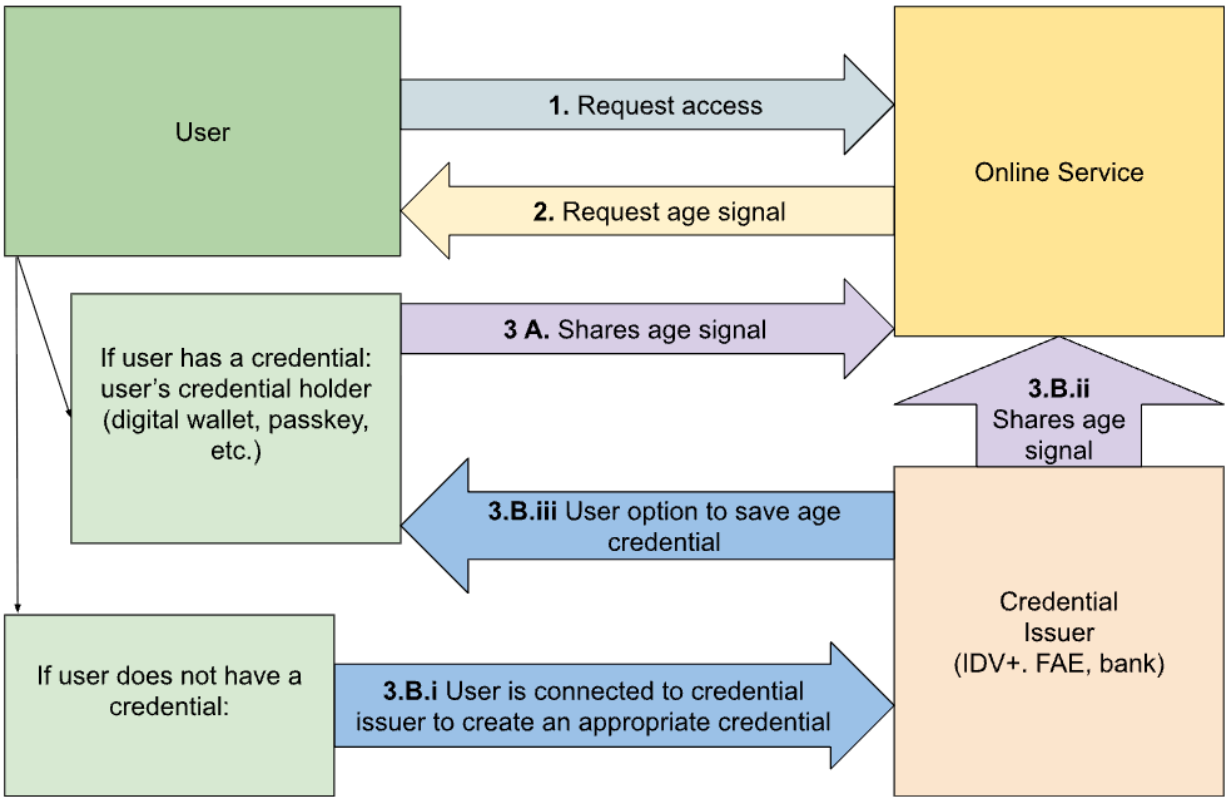
At the state level, several states have actually passed bills that will go into effect over the next year or two that are similar in approach to the federal proposal, although it is likely that lawsuits will challenge the new laws.

A way forward

While we acknowledge the appeal of efforts like a blanket app store or device level requirement, we think it is timely to offer an alternative approach and rationale that balances safety and privacy. This approach would recognize that conducting age assurance in connection with all apps is not necessary.

A better way forward is an age assurance approach that creates obligations that are proportionate to the risk and an approach that is sensitive to the nature of the content and experience of an app, website or platform. This would draw on existing tools and methods that tech companies themselves have already developed and that are continuously being improved.

While everyone has a role to play, responsibility lies with the apps, websites, and platforms to take steps to ensure that their products and services are accessed by users of an appropriate age.



How it works

Here are two potential scenarios:

➡️ A digital adult tries to access an 18+ website. At the home page, the user is confronted by an interstitial screen asking them to attest that they are over 18. Once they answer yes, they are further required to provide proof that they are, indeed, an adult by directing them to a credential issuer, or to provide a credential that they already have in a credential holder. Once this is provided, they are allowed access to the site.

➡️ A digital minor wants to set up a social media account. They are asked to attest that they are over 13. Once this is done, a follow up screen asks them for a credential stating that they are of age to use the app. They are offered several credential options. Once the teen has completed the respective tasks needed to get a credential they submit this to the social media platform and they are allowed to set up an account.

The illustration above is a flow chart showing examples of how this process could work, both for a user going through the credential creation process for the first time, and then using a credential holder in the future.

A user tries to access an app or online platform. If that platform/app falls into a certain risk profile, the platform/app asks for the user's age. There are a couple of ways that a user could then provide their age, depending on the platform/app, the level of risk, the device and operating system, where the user lives, and more.

A trusted privacy-preserving piece of technical infrastructure could share a user's age range (such as through Apple's Declared Age Range API), or share an existing age credential saved on a user's device (such as a government ID stored in a Google Wallet), or additional methods that are being brought on stream. A platform/app can also contract directly with a credential issuer (such as Instagram using Yoti for facial age estimation). There should be some Trusted Privacy Preserving infrastructure between the content provider and the credential issuer, but a provider might choose to integrate directly with a credential issuer rather than a credential holder if it makes sense to do so for their users and content.

Upon reviewing a user's credential, the platform/app can then allow access and provide an age appropriate experience. Our approach highlights multiple acceptable options for age assurance processes that are consistent with the principles listed above.

Conclusion

By anchoring age assurance in proportionality, privacy, and shared responsibility, we can protect children online without sacrificing innovation, free expression, or user trust. This is not a call for a single silver bullet solution, but for a flexible, interoperable framework that adapts to risk while safeguarding rights.

October, 2025

Appendix

Definition of terms

Here is a brief set of definitions of the terms used in this paper with examples:

1 Credential

Definition:
A *credential* is a digital (or sometimes physical) attestation that verifies a specific attribute about a person. In the context of age assurance, a credential is a privacy-preserving attestation that verifies a specific attribute about a person - such as being under 18, over 13, or a parent/guardian - without exposing their identity.

Example:
An age credential is verified via an age assurance or age verification service which states “this user is 18+”.

2 Credential Issuer

Definition:
A *credential issuer* is a trusted entity that creates verified age assurance credentials. The issuer validates the user’s information and issues a credential.

Example:
An ID verification service verifies that the image of a driving license matches the individual presenting that ID, and that the ID is valid and the details are correct. The ID verification service then issues a credential that the user is, for example, 18+ (i.e. not specifically how old they are, but that they pass a threshold age.)

3 Credential Holder

Definition:
A *credential holder* is the trusted infrastructure that securely stores and enables access to the credential. The credential holder, with the user’s permission, shares the credential with apps and platforms in order to access age appropriate online experiences.

Example:
A 16-year-old using their mobile phone to present a digital credential that confirms they are under 18 in order to access an age-appropriate version of a platform.

Assessing levels of risk

There is existing guidance for platforms to assess the level of risk their products and services fall into. Regulators and organizations have produced guidance, including the UK's Ofcom[1], Unicef and the Danish Institute for Human Rights[2], and Unicef and the BSR[3].

1 https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/risk-assessment-guidance-and-risk-profiles.pdf?v=390984

2 https://www.unicef.org/childrightsandbusiness/media/541/file/Childrens-Rights-in-Impact-Assessments.pdf

3 https://www.bsr.org/reports/BSR_UNICEF_D6.pdf