Discussion paper

Where in the tech stack should age assurance sit and how should it be done?

January 2025

Author

Julie Dawson,

Chief Regulatory and
Policy Officer at Yoti

Where in the tech stack should age assurance check(s) occur?

Should they be on device on a software as a service (SAAS) basis, at operating system level or at more than one level in the stack?

How and where should the age assurance be retained?

Age assurance technologies have evolved significantly over the past decade, with approximately 50 organisations developing tools ranging from age verification to age estimation and inference. Some of these tools are now independently audited and comply with global standards. There's also benchmarks like the National Institute for Standards & Technology (NIST) evaluation of AI facial age estimation. These approaches are designed to minimise consumer burden and be simple for organisations to integrate, within a matter of hours.

In this discussion paper, we explore where age assurance checks should sit in the consumer journey and in the tech stack; if it should be a **one-off check** at set up or **both** at set up **and** at the **point of accessing** a service, for added safeguarding. We will explain how tokenisation can lower the cost of repeat checks. Another approach described is a **layered approach** to age assurance combining:

- Age verification during device setup.
- Periodic reauthentication at the device level.
- Age checks at service access points.

However, we need to reflect, with the approach selected, does this really create more burden or less on parents and does this safeguard young people and deliver age appropriate access and experiences?

Yoti's view, weighing the factors discussed in this paper, is that the optimal placement of age assurance within the tech stack and consumer journey depends on

✓ **Balancing consumer convenience**

✓ **Privacy**

✓ **Operational feasibility**

1. https://accscheme.com/registry/
2. https://avpassociation.com/standards-for-age-verification/

Principle of proximity

We advocate that to enhance consumer understanding and acceptance, age checks should occur as close as possible in time to the relevant activity or service which requires age appropriate access. For example, at the very point in time when signing up for a gambling, adult content or dating site platform it is logical that the check is at the direct point of access. This ensures underage people can't access these platforms and content. In the case of a mixed age service such as gaming; this allows a differentiated service to be offered to minors. This principle of context-specific implementation is designed to make it clear to users why they are undertaking the check.

Interoperability and reuse - tokenisation

It stands to reason that once you're clearly over 13, 18 or 21 - you're not getting any younger. So once you've passed an age threshold, you don't want to have to keep repeatedly proving that you have reached that age threshold.

The flip side for regulators and platforms is that they want to be sure that it really is the right person who is accessing a service and not a proxy access, that may have been paid for, to bypass the age check.

To meet this issue and to reduce costs across industries, age verification providers have established interoperable, tokenized approaches. Users can verify their age once and gain continued access to a number of platforms for a certain time period, as approved by regulators, according to the use case and the risk profile. For example, an 18+ token from an adult content site can be reused across other services like dating or gaming platforms, for a certain period.

Binding successful age verification to passkeys saved on device is another way to strengthen repeat authentication.

Parental role and challenges

Many platforms have invested heavily in devising elegant and thoughtful parental controls, no doubt with good intentions. However, despite this, most parents struggle with setup and management of parental controls. This may be due to children pestering them, peer pressure, children outwitting them, or the technical complexity and time required to set up the controls across multiple devices and services.
Industry data shows minimal parental control adoption—for instance, only 1% of U.S. parents use Snapchat and Discord parental control tools.[3] This reality underscores the need for system-level solutions; rather than solely relying on a parent in the loop to set the age of their child within the set up of every device.

[3] U.S. Senate Judiciary Committee hearing in January https://www.techpolicy.press/transcript-us-senate-judiciary-committee-hearing-on-big-tech-and-the-online-child-sexual-exploitation-crisis/https://www.nbcnews.com/tech/social-media/fewer-1-parents-use-social-media-tools-monitor-childrens-accounts-tech-rcna145592

Proportionality of burden or friction on adults

One of the key considerations in the US has been: is the age assurance journey overly burdensome to an adult? It is worth considering the user experience of unboxing a new phone. Today, when you unbox your new device it is relatively straightforward to set up your new phone, though still some people struggle. And data transfer can take a few minutes to a few hours, depending on the storage on the old and the new phone. However, adding additional friction of undertaking an age check at the moment of unboxing may be unpopular.

In this future world of operating system age checks, you would in addition be asked to go through an age verification, age estimation or age inference check, of your choice. Depending on the options available to an individual, that could take from a few seconds to minutes to a couple of hours.

But this highlights some questions, including:

- How could that be made mandatory across all devices globally?
- Would the device be locked down until an age check had been undertaken?
- Whilst parents may set up devices for young children; teens may unbox their own new devices if they've already had one for several years..
- Given that there are hand-me-down devices in families; would a subsequent re-authentication be required to ensure that the person using the device is actually the same as the one who undertook the initial age check?
- How often should re-authentication be required?
- How would this be relied on with open-source operating systems? (For instance Linux is open source, so it is conceivable that any operating system level age verification can be disabled or modified by the user of the system to generate false results)
- Who is responsible for preventing the age verification information being used by predators to target minors?

There are now calls from certain industries to consider undertaking checks at other levels in the tech stack, including device-level age checks. In the next section we try to outline some of the practicalities as well as the positive and negative, intended and unintended consequences of these suggestions.

System-level age checks: pros and cons

By system-level age checks, we mean Operating System (OS) and App Store Integrations.

Pros

- Streamlined process and reduced burden on smaller organisations.
- Potential to provide a level playing field in terms of regulation.

There are suggestions that age checks at Operating System or App Store level could streamline the process and reduce the burden on certain sectors, perhaps for the long tail of smaller organisations. This has appealed as a concept to some large organisations who want a ‘level playing field’ in terms of regulation, so it is not just the largest players who are required to undertake age checks. The main proponents of this suggestion are adult content and social media organisations. There is little detail given however, as to how this would happen in practice.

Implementing age assurance at the operating system or app store level raises some practical and ethical questions, which we outline below.

Cons

- Sector exclusion: certain goods and services (e.g., alcohol, nicotine) are not present in app stores.
- Burden on parents to set age levels for every device.
- Device reuse and resale introduce complexities in maintaining accurate age assignments. (For instance hotel rooms, holiday apartments with smart devices - would these be locked by the hotel management and require adults to request family controls be temporarily removed?)
- Device sharing across family members i.e. iPad used by both parents and children.
- Risks of data exploitation and breaches.
- Cost of delivering the service and concerns about corporate dominance.
- Increased complexity for app stores, requiring partnerships with third-party providers.
- Privacy and data risks:
    - Centralised age verification at operating system level may collect sensitive data, increasing the risk of large scale data breaches.
    - Sending age signals from app stores to apps raises tracking and privacy concerns.
    - Anonymous access to apps may be undermined by mandatory age verification.
- Where low cost devices are not supported, in terms of operating systems with age verification enabled capabilities, the device owners may be priced out of content access.
- Legacy devices remain in circulation for many years

- **Sector exclusion:** Adult content is absent from app stores and age-restricted goods, such as alcohol, nicotine and vaping, are purchased online or in-person. How would operating system or app store level checks work across these goods and services?

- **Burden on parents:** Is this really coded language for 'the parent has to set the age of every device in the household'? If only a small percentage of parents are managing to set up parental controls on the most popular social media platforms, can we expect parents to manage resetting the operating system age levels across multiple devices in the home? How is a child supported if their parent does not engage with setting the age at an appropriate level?

- **Device reuse:** How can a platform or a network operator check that age is reassigned when devices are handed down in the family or resold?

- **Device estate**: How to deal with the existing estate of billions of legacy devices, how could they be required to incorporate operating system level age checks?

- **Data exploitation risks:** The data in question - identity or age - also potentially has value for the organisations that access it. Centralised age and identity data might tempt companies or bad actors within companies to turn a blind eye to data minimisation requirements and harvest or monetise personal information despite risking privacy or security violations.

  One of the attractions of independent age verification providers has been that their contracts are predicated on not reselling the age or identity data to third parties, or using that data to mine or build personalised products and services.

- **Data centralisation risk:** Age verification at operating system level may include verification, estimation or inference approaches and may lead to the centralised collection of sensitive personal data, such as birth dates or ID's, which these platforms may then also store, increasing the risk of data breaches, unauthorised data mining and misuse.

- **Managing redress:** How to manage redress, when people are given the incorrect age? Additionally, how do you periodically check that the right person is still using the device? What ongoing re authentication is deemed proportionate by data protection regulators?

- **Cost of delivering the service:** Who should pay for the operating system level checks? Should those offering operating systems be forced to provide them pro bono - is that fair? How should this service be charged for - the initial assessment of age, ongoing customer support, and any reauthentication? The balance between service quality, sustainability and service monetisation must be carefully managed. However, the app stores or operating system organisations may offer a trade - we will provide this age assurance service for free or at this price; however the quid pro quo, is that we wish to mine and reuse this valuable data. Would this be deemed fair by regulators and the public?

- **Market and regulatory considerations:** Competition authorities around the world keep a close eye on platform monopolies. If age assurance is done at operating system level, this could deepen concerns over corporate platform dominance. It is fair to say that much of the innovation, in terms of age assurance, has not stemmed from the large platforms or from the operating systems level organisations. Will continued innovation in age assurance flourish if a small number of operating systems undertake the bulk of checks globally? How will regulators audit the quality of their work? Would operating systems be required to meet the incoming international standards for age assurance? Would dominant global platforms be allowed to charge whatever fees they like for age checks or would pricing have to be regulated? Would age be a Trojan horse for dominant platforms to then dominate the identity market and would their identity fees need to be controlled by competition regulators?
  In sectors such as online gaming, there has been an uneasy relationship between the app stores and gaming sector; where the cost of access / fees charged by app stores has been a bone of contention.
  There has also been concern over the prospect of supra national identity systems, not owned by national governments, but by global corporations. Identity data is closely linked to payments data; so access to that data, would provide a strong competitive advantage to any organisation able to leverage that.

- **Cost and operational burden:** Implementation requires significant financial investment, affecting both app developers and users. It is not just the technical solution that would require investment to develop and maintain. There will also be a requirement for customer service, support for app developers who need to confirm age ranges, and associated legal and compliance costs, transparency audits and requests for information when either data protection or content regulators conduct periodic audits. There is a liability risk; the operating systems would need to consider when undertaking their pricing, that they could face reputational and legal risks if their systems fail, whether by incorrectly verifying ages or being exploited to bypass safeguards.
  Yet, there is no doubt that providing the service of ascertaining age requires investment to provide a secure and robust check; in potential rechecks, in customer support for dispute resolution with consumers, and subsequent audit by regulators. So at whichever level in the stack an age check is undertaken, it will not happen without a sustainable business model.

Shift of accountability

Accountability may shift in other directions for instance to parents if they have to setup or remove restrictions.
Shifting age assurance responsibility to app stores may reduce accountability for developers, who are better positioned to implement tailored systems.
Do relying parties for example hotel or leisure facility management become accountable for children using their facilities to access services such as adult content (pornography)? Likewise, does any company / work environment become accountable for a child accessing adult content if the child is using company equipment that could or should be locked and age verified?

Device-level age checks

Device-level checks can address specific contexts but face practical and ethical challenges:

- Trust in device security and assurance against data leakage.
- Risks of unauthorised image capture and data sharing.
- Challenges in maintaining privacy and ensuring robust re authentication mechanisms.
- Device reuse poses significant challenges in family and resale contexts.
- Reliance on device manufacturers for ongoing compliance and auditing of practices.

Device-level versus user-level challenges

- Age settings applied at the device level may not suit multi-user households, leading to excessive restrictions or unintended access.
- Individual account-based verification is more flexible but may require more complex implementations.

First of all, it's worth being clear as to what is meant by 'device level'. Device level checks could be construed to be solely consumer devices - handsets, games consoles, VR (virtual reality) headsets etc. Or device level checks could also be considered to be on any hardware device including in store hardware - such as gambling terminals or electronic point of sale cash points in store.

Many age assurance approaches already use encryption, threat monitoring and minimal data retention, ensuring a high level of security. Given this, requiring additional on-device processing for age checks may be redundant. While on-device checks might be suitable for specific contexts, like retail terminals, broader implementations should leverage secure cloud-based verification to avoid unnecessary device-level complexity and maintain privacy safeguards.

In the case of device-level age checks, there are further complexities:

- A relying party would have to trust that the device has not been compromised and to rely on the response from the device. A device based approach allows a device to undertake multiple attacks.
- Parents may input false age information to bypass restrictions under pressure from children.
- Where age controls are tied to devices rather than individual accounts, this provides less flexibility and may fail to address the nuanced needs of multi-user scenarios.

There must also be a level of trust with the on-device provider, relying party and consumer that any images captured by the device are not stored or shared. Without auditing it is not possible to be sure that an on device offering does not deliberately share or unintentionally leak personal information.

Is a one-off check at set up sufficient?

This begs a further question; in the instance that the operating system check has failed as the device is no longer in the hands of an adult, what other protections are in place? Take for instance the scenario of a 3 year old child whose parent does not set up their age as a child, but as an adult from the outset.
Another suggestion is to not just have a one-off check at set-up; but to also have an age check at the point of access

Layered checks both at set up and an additional check at the point of accessing a service

This could lead to a layered set of 'just in time checks' so both at set up and an additional check at the access point of say an age-restricted service, such as live chat in gaming or 18+ gambling, dating, adult content.
Stage one could be to bind age checks to passkeys and integrate mandatory age verification during device setup. And then subsequent periodic reauthentication could be required at device level. This could be supplemented by checks at the point of access of various services.

Potential unintended consequences

- Some apps and services may exclude minors entirely to avoid regulatory burdens, depriving them of safe online experiences.
- Increased friction in app downloads could discourage legitimate users.
- There could be complexities if the operating system level or device level age verification is different to a subsequent point of access age verification (i.e. because the device is being reused or shared) then would other services that rely on the historic app store age or device age be stopped?
- Small developers may struggle to meet certification requirements, stifling innovation and competition.
- Parents could face more rather than less complexity.
- Global platforms may face challenges in adhering to varying local regulations.

By requiring a layered approach, with more age checks than is the current requirement, this may lead some platforms to decide to only provide their services to adults and no longer service the youth market, thereby reducing the offerings to young people.
By requiring age assurance at several levels in the stack, this could also alienate users and discourage adoption. Parents who are already struggling to deal with parental controls, may give up on supporting operating system controls as well as parental controls, if they are perceived to be an additional complexity and burden.
Additionally, whilst larger operating systems and organisations may adapt to meet requirements; smaller organisations may struggle.

These are nuances that have not been discussed widely though.

Conclusion

The optimal placement of age assurance within the tech stack and consumer journey depends on balancing consumer convenience, privacy, and operational feasibility.

Today’s approach is to undertake age checks ‘at proximity’ at the point where a user accesses a service. This is working now and at scale. There are billions of such age checks being undertaken annually; following international standards, which can be audited by independent accredited audit bodies. The more this develops across age restricted sectors, the lower the cost for all the industries involved. These approaches can be tokenized, with each token lasting for a limited time. There can be regular authentication to the current user of the device.

A future, multi-layered approach could be devised, which extends the number of places where age checks are undertaken. This type of approach would need to consider service-specific context, minimise data sharing, and align with global standards for age assurance that offers the most robust path forward. However this will take time to think through. We need to avoid creating an even more complex environment for parents and ensure that users understand the rationale for any change.

The existing age assurance industry, which has decades of experience in delivering independent and auditable approaches, is keen to support regulators to think through the practicalities as well as the positive and negative intended and unintended consequences of the sweeping statement to ‘undertake checks at operating system level’.

Age checks are already required by law now, and there are approaches available that meet the requirements. Before, in one penstroke demolishing what exists today, a thorough review of the questions in this paper is recommended.

YOTI

To find out more visit **yoti.com**