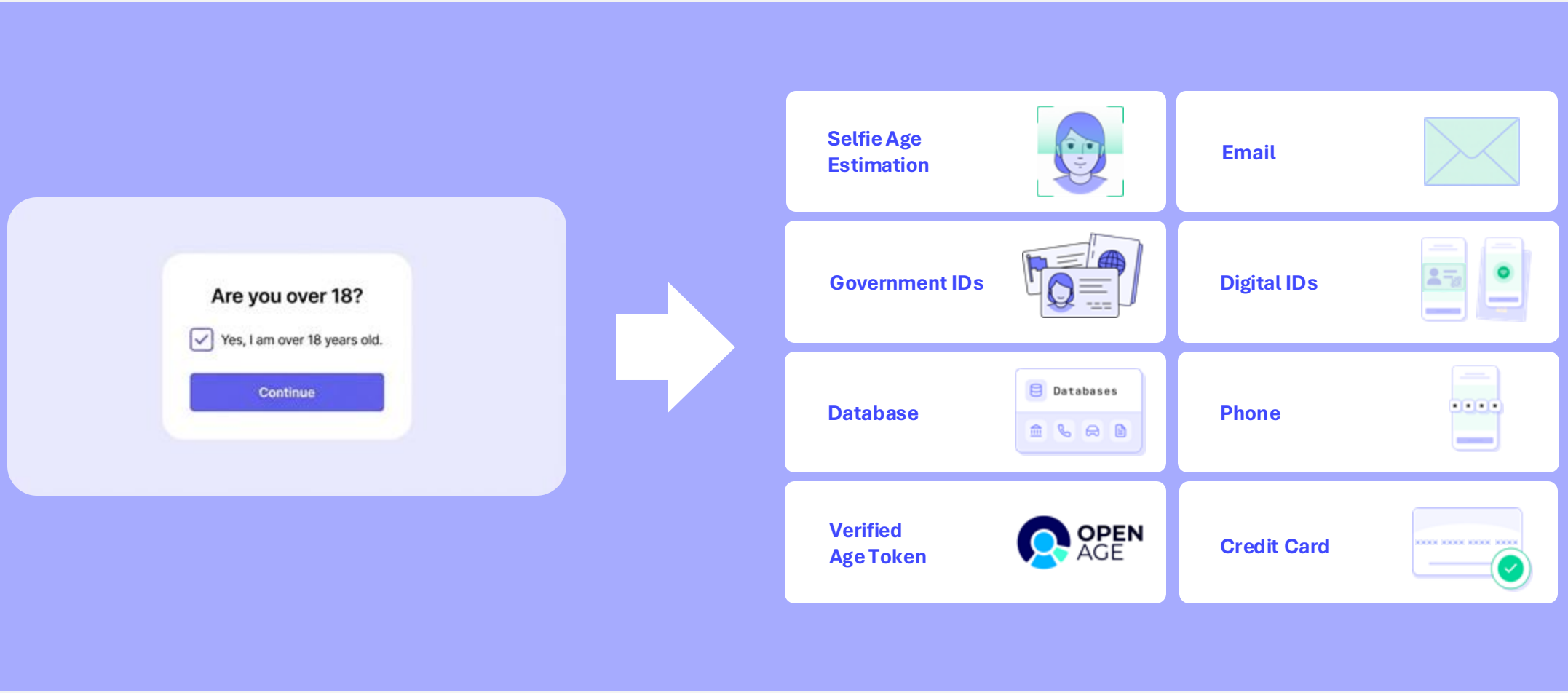
Performance learnings from deployed age assurance technologies

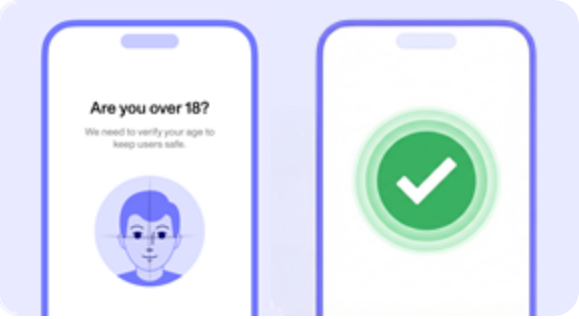
Moving past self-declaration of age

Because declaration is easy to circumvent, other age assurance technologies are being adopted.



Technology assessment framework

Performance metrics to help evaluate what technology is right for the use case



Coverage

Proportion of the population that can leverage this technology

Assurance

Level of confidence that the user is the age they claim to be

Usability

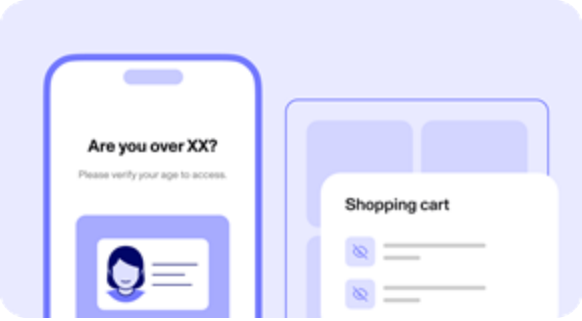
Ease of use for users to perform check

Different age goals need different approaches

Adult access control and kid-safe online experiences require different approaches

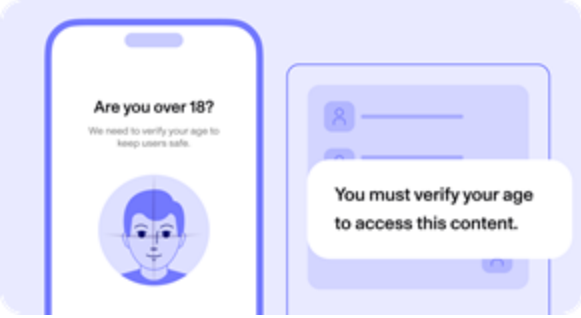
Age Gating (Age ≥ 18)

Protect children from accessing inappropriate content/services



Age-Restricted Services

Inappropriate Content



Age Appropriate Experiences (Age < 18)

Ensure children have safe online spaces

Online Communities

Multiplayer Games

Comparative performance of technologies

Depending on age goal, technology performance varies on coverage, assurance, and usability

Age Gating (Age ≥ 18)

Technology	Coverage	Assurance	Usability
Selfie age estimation	High	High	High
Government ID	High	High	Medium
Phone	Medium	High	Medium
Email	Medium	Medium	High
Credit Card	Medium	Medium	Medium
Database	Medium	Low	Medium
Digital IDs	Low	High	High
Reusable age token	New		

Age Appropriate Experiences (Age < 18)

Technology	Coverage	Assurance	Usability
Selfie age estimation	High	High	High
Parental consent	High	Medium	Low
Government ID	Medium	High	Medium
Digital IDs	Low	High	Low
Reusable age token	New		

Age Gating (Age ≥ 18)

Commonly attempted circumvention techniques

Parental Impersonation

Handing device to parents to verify selfie under false pretenses

Borrowed Government ID

Genuine IDs that are borrowed from an older acquaintance

Location Spoofing

Spoof location to countries that do not require age assurance

Age Gating (Age ≥ 18)

Proven techniques to stop circumvention

Parental Education

Design experiences to clearly warn parents the intent of verification

Proof of Ownership

Verify the individual and their ownership of the government ID

Spoofing Risk Signals

Leverage behavioral, device, and network signals to determine likely location spoofing

Age Appropriate Experiences (Age < 18)

Commonly attempted circumvention techniques

Deepfakes

Leverage AI to generate synthetic faces masks to impersonate minors

Account Selling

Uptick on shared accounts based on some limited device information across accounts

Fake Parental Consent

Improper attestation from an adult with no parental relationship to an impersonated child

Age Appropriate Experiences (Age < 18)

Proven techniques to stop circumvention

Multimodal Fraud Defense

Adopt multimodal approaches to prevent fraud and test against 3rd-party assessors

Continuous Verification

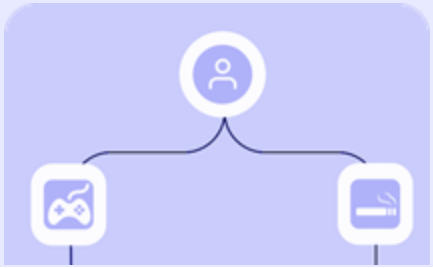
Verify that the individual is the same owner when anomalous behavior is detected

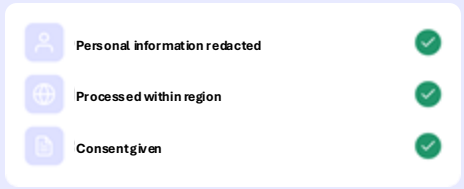
Parental Relationship Proof

Verify the parent and establish proof of relationship ideally through child-in-the-loop confirmation

Privacy must be considered upfront

Appropriate data handling and usage is crucial to protect children’s right to privacy





Age Appropriate

Assess whether an age assurance method is appropriate given the demographic.

Risk Appropriate

Assess goals to ensure the method is appropriate for the given use case and context – risk of child accessing adult content vs risk of adult posing as a minor.

Data Management

Assess data management policy to ensure that data is being redacted as soon as possible.

Data Minimization

Assess the minimum amount of data collected and stored to achieve the use case, and align with data minimization principles as referenced by GDPR, ISO/IEC 27566-1.