UNPACKING AGE ASSURANCE: TECHNOLOGIES AND TRADEOFFS

Age Assurance is the broadest term for methods to discern the age or age range of an individual. There is no one-size-fits-all method, and it is important to consider context to determine a proportionate method of age assurance for each specific use case. Proportionality is key because in some contexts, a higher level of certainty is appropriate. This must be carefully balanced against the privacy risks and risk of barring access to legitimate content - especially if content restrictions have inequitable impacts. It may be appropriate to employ multiple methods in a layered approach.

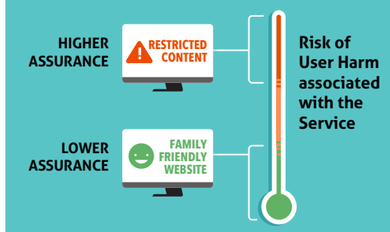
FUTURE OF PRIVACY FORUM

AGE ASSURANCE QUESTIONS

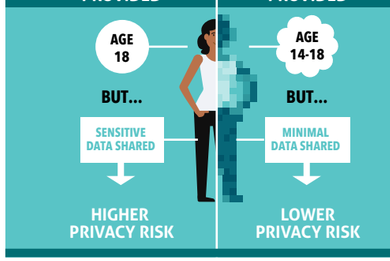
WHAT ARE THE GOALS?
- Facilitate parental consent
- Limit access to an age-restricted service or provide age-appropriate content
- Verify an individual's exact age
- Place individuals within an age band (e.g. 13-15)

WHAT ARE THE POTENTIAL HARMS TO MINORS?
Harms could include children or teens accessing age-restricted services, content, or contact by unknown individuals.

WHAT IS THE APPROPRIATE ASSURANCE METHOD?
Choose a method or methods that provides a level of age assurance (accuracy) proportional to the goals and risks of the service, keeping in mind that legal obligations may dictate a specific method.



IS ASSURANCE BALANCED WITH PRIVACY RISKS?
After considering privacy risks and mitigations, confirm that the assurance goal warrants the level of privacy risks and other impacts associated with the chosen age assurance method.



COMMON EXISTING & EMERGING METHODS

DECLARATION

AGE GATE

A user indicates their birthdate without providing supporting evidence. This common method is most appropriate in low risk situations, as children and teens frequently bypass by providing a false birthdate. Privacy risk is low, especially if birthdates are not retained or matched with a name or other indirect identifier.

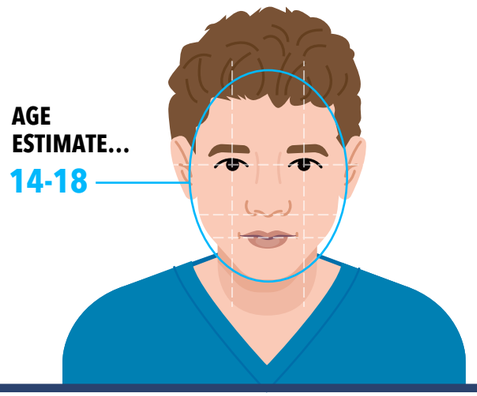
PARENTAL CONSENT/VOUCHING

A parent with a verified account (e.g. using government ID, credit card, etc.), declares the child or teen's age by providing consent or adding the child to their account. This has higher assurance than an age gate, but may impact the teen's autonomy.

ESTIMATION

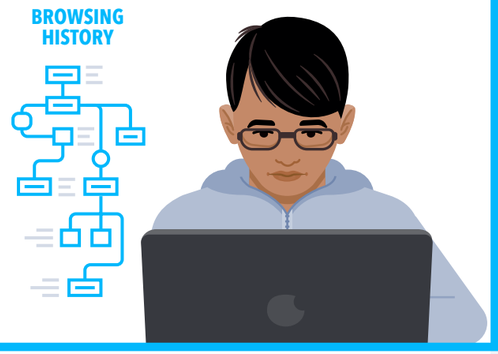
FACIAL CHARACTERIZATION

Estimates age using a facial image, but the individual is not uniquely identified. Best used to place users in age bands, or signal that a user meets an age threshold, such as under 13 or 21+. Estimation is less effective for discerning age in a narrow range like 17 vs 18.



OTHER ALGORITHMIC ESTIMATION METHODS

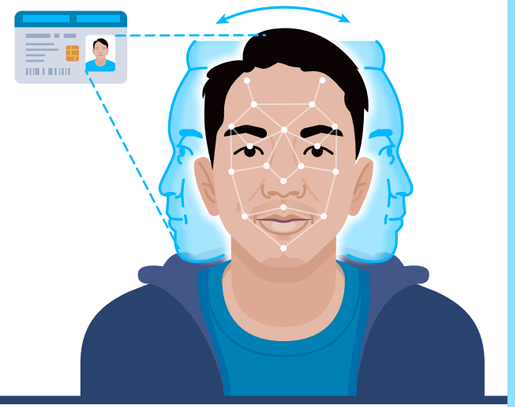
Other algorithmic methods could include estimation of age or age range based on browsing history, voice, gait, or using multiple data points or signals from a VR game.



VERIFICATION

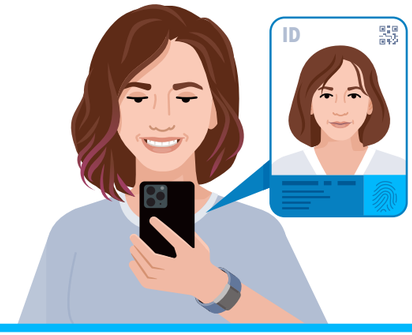
BIOMETRIC + GOVERNMENT ID

Matches a scan of a government-issued ID and live photo or video using facial recognition. This method is more appropriate for higher risk, regulated or age restricted services. Government ID only is another method, but provides less assurance.

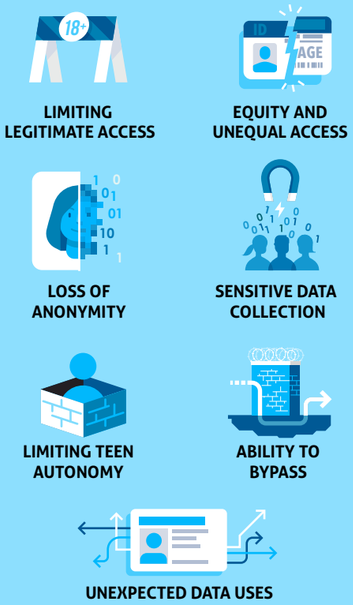


ON DEVICE DIGITAL ID/WALLET

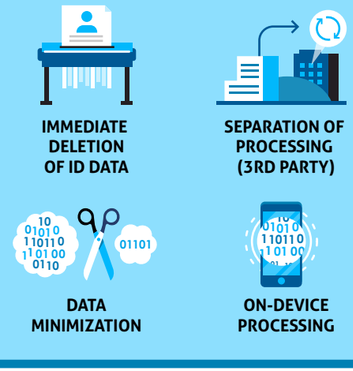
Using a wallet app, users add one or more verified credentials to create a reusable digital ID stored either on device or in the Cloud. Users verify their age with the service by inputting a code to share details required for age assurance (e.g. 18 or over).



RISKS OF AGE ASSURANCE



RISK MANAGEMENT TOOLS



EXAMPLE USE CASE

AGE ASSURANCE FOR ONLINE GAMING

In this scenario, Miles, a 16 year old, is accessing an online gaming service that is designed for teens and older. It has optional age-restricted features.

INITIAL EXPERIENCE

DECLARATION

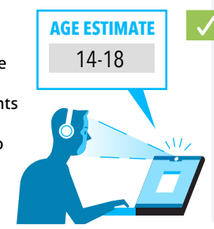
The default user experience is "teen-friendly," Miles can sign up by providing their birthdate.

ASSURANCE
PRIVACY RISK

SECONDARY FEATURE

ESTIMATION

Later, Miles wants to enable a feature which the game developer has restricted to 16+. The developer wants a higher level of assurance. A "live selfie" uses facial characterization to determine Miles is between 14-18.

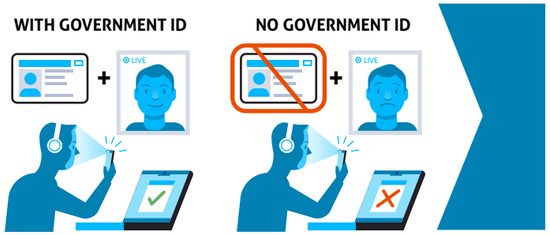


ASSURANCE
PRIVACY RISK

GREATER ASSURANCE NEEDED

VERIFICATION

Because the estimated age range includes ages that aren't allowed to use the feature (14-15), greater age assurance is needed. Miles must scan their driver's license and take a "live selfie." However, many users, including 75% of 16 year olds, do not have a driver's license.



ASSURANCE
PRIVACY RISK