Design Codes, Privacy & Age Assurance (V. 1.0)

- **Design Codes improve privacy, they do not harm privacy.**

Design Codes are drafted to improve the privacy of young Americans. For example, Design Codes require that companies:

- Make their privacy notices 'plain speak' and easy to read, so we understand what they do and can make better decisions about which apps and websites to use
- Provide easy to use, responsive tools that allow children and parents to make a complaint if something has gone wrong with their privacy
- Stop using 'dark patterns' to trick users into handing over more data when they sign up to a service
- Stop companies collecting unnecessary geolocation data
- Stops companies selling and sharing kids data unnecessarily
- Undertake a Data Protection Impact Assessment about their product, which includes identifying potential privacy risks and mitigating against them
- Default users accounts to 'the most private settings' if those accounts belong to young people, or they're not sure of the user's age

Many of these provisions and services might improve privacy for people over 18 too.

- **Design Codes do not automatically require proof of ID.**

Design Codes do not call for automatic age verification, nor will every platform have to check your ID to open an account. This is a 'falsehood' often peddled by opponents of the Code.

Design Codes require digital services to determine the age of their young users "*with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business or apply the privacy and data protections afforded to children to all consumers*".

Age determinations need to be proportional to the risks a service presents. This means two things:

1. If companies are safe, always handle data in secure ways and default all users to strong privacy settings, they *do not need to estimate or verify users' age at all*. Simple.
2. If companies want to use data in risky ways, they need to balance the level of risk with the level of certainty they need about a user's age. For example, if they publish people's locations live for anyone in the world to see (a very risky practice!) they might need very strong age *verification* techniques like seeing ID. If their practices are less risky, like publishing pictures of users online for only approved friends to see, they can use lighter age *estimation* techniques like asking users their age and checking this with a 'trusted adult'.

The same requirement exists in the UK, Ireland and multiple other countries. Users do not need to verify their age by providing ID to use websites or social media platforms in these countries.

- **If companies need to know a user's age, there are many techniques available that have limited privacy impacts.**

If a company wants to continue to use data in risky ways, and so need to assure themselves of a user's age, there are lots of privacy preserving ways to do this. This includes *estimating* age by;

- Asking users to enter their age (or asking twice, if a child made up a fake date of birth they may forget it the second time). This is often called self-verification.
- Asking users to get an adult or two to vouch for their age, by sending them a simple link to confirm. This is often called social vouching.
- Using data the companies already analyze to estimate the age range of users, such as data about what videos they watch
- Age estimating AI, that very accurately estimates the age of a person using a selfie (the selfie and data is then deleted). This is common and is already being trialed by Instagram[1].

Services that choose to be risky need to determine a user's age with a level of certainty that is closer to *verification*. Depending on the risks involved, this could be done with credit cards, third party age verification service, age tokens or other forms of IDs (as some online services already do, like gambling sites).

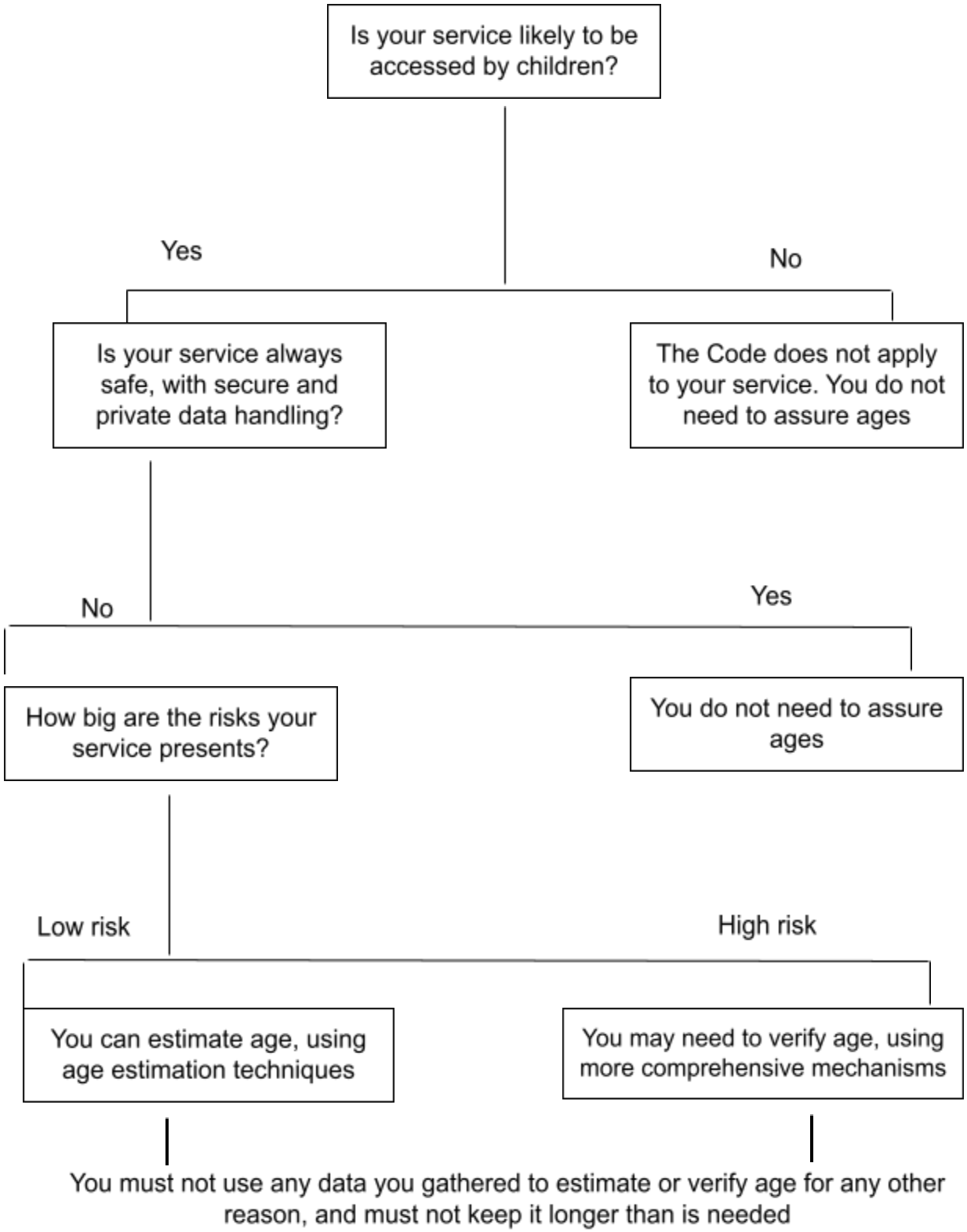
Where services determine age, the Code makes clear that any data collected only to estimate or verify ages cannot be used for *any other purpose, or retained for longer than is necessary.* They simply see any proof of age, note that they have determined your age, then delete it.

- **Age estimation or age verification? What's required?**

Age assurance under the Code needs to be 'risk based'—the amount and type of data that is collected about a user's age needs to be balanced against the risks their services pose. Where the risks are deemed to be low, age assurance techniques can be used to reliably *estimate* age (like self verification, social vouching, age estimating AI etc). Where the risks are higher, they may need to *verify* a user's age with stronger techniques, like using credit cards, third party age verification services, age tokens or credit card details. They cannot use this information for anything else, and cannot retain this data for long.

[1] https://about.instagram.com/blog/announcements/new-ways-to-verify-age-on-instagram

‘Strong’ age verification is unlikely to be the most common scenario



- **Who decides if a service is low or high risk, or if they need to age assure?**

Services that children are likely to access have to complete a Data Protection Impact Assessment. This identifies all the risks that emerge from the way they collect and use young people's data, and documents strategies to mitigate these. The Code identifies at least seven considerations for a Data Protection Impact Assessment, including: exposure to harmful features or content; allowing children to be targeted by harmful contacts; ability of children to experience harmful conduct; ability of children to be exploited etc. This helps to describe and determine the overall risk profile of a product or service.

This risk profile informs the decisions by companies about the need to age-assure their users, and companies would need to document their decisions. This should include which approaches and techniques are deemed most appropriate, given the risks identified.

Impact Assessments must be reviewed at least every two years. State Attorneys General are able to request to see these Impact Assessments, and can take curative steps with companies where they believe their risk identifications or mitigation strategies are insufficient.