



Submission to the Age Assurance Technology Trial

May 2025

Company Name: *Meta*

Solution Name: *App store/OS level age verification*

Lead Contact: [REDACTED]

Lead Contact Email: [REDACTED]

Lead Contact Phone: [REDACTED]

Executive Summary

Meta appreciates the opportunity to make this submission to the Age Assurance Technology Trial on the potential for a ‘whole of ecosystem’ age assurance approach to addressing the many and growing concerns of policy makers and parents for greater age verification.

At Meta, we invest significantly in providing people, especially young people, with an age appropriate experience on our services. The privacy, safety, and wellbeing of young people on our platforms is essential to our business. Our policies prohibit problematic content, including content or behaviour that exploits young people, and we work closely with experts in mental health, child development, digital literacy and more to build features and tools so that teens can connect online safely and responsibly. We continue to make ongoing investments in this space.

In September 2024, we announced the introduction of Instagram Teen Accounts in Australia to automatically place teens in built-in protections and reassure parents that teens are having safe experiences. Teens under the age of 18 will be automatically placed into Teen Accounts,¹ and teens under 16 will need a parent’s permission to change these built-in protections to be less strict. Early teens (aged 13-15) will be automatically placed into defaults, for example, a private account, messaging restrictions, the strictest setting of our Sensitive Content Control,² a daily limit reminder after 60 minutes of use and no notifications from 10pm to 7am. If an early teen wishes to change to a less protective setting, they will need to set up a supervision relationship with their parent/guardian and seek parental permission to make that change.

Understanding a user’s real age is key to all of the efforts by policymakers and app providers to promote a more age appropriate experience online. However, if an app-by-app age assurance approach is adopted, then parents and young people will face considerable time, privacy and security impositions to engage with the age assurance approach adopted by each app. There is a simpler way: a ‘whole-of-ecosystem’ approach that requires app store and OS providers to share age bands APIs with app providers – information which, we believe, is already being collected today.

Given our submission outlines a technical solution that is not in existence today, and is not a solution that neatly maps to the requirements outlined in the Practice Statement, it is not possible for us to provide it in the precise format required. We have, however, sought to address as many of the key requirements of the Practice Statement as possible.

¹ Meta, ‘Introducing Instagram Teen Accounts: Built-In Protections for Teens, Peace of Mind for Parents’ <https://about.fb.com/news/2024/09/instagram-teen-accounts>

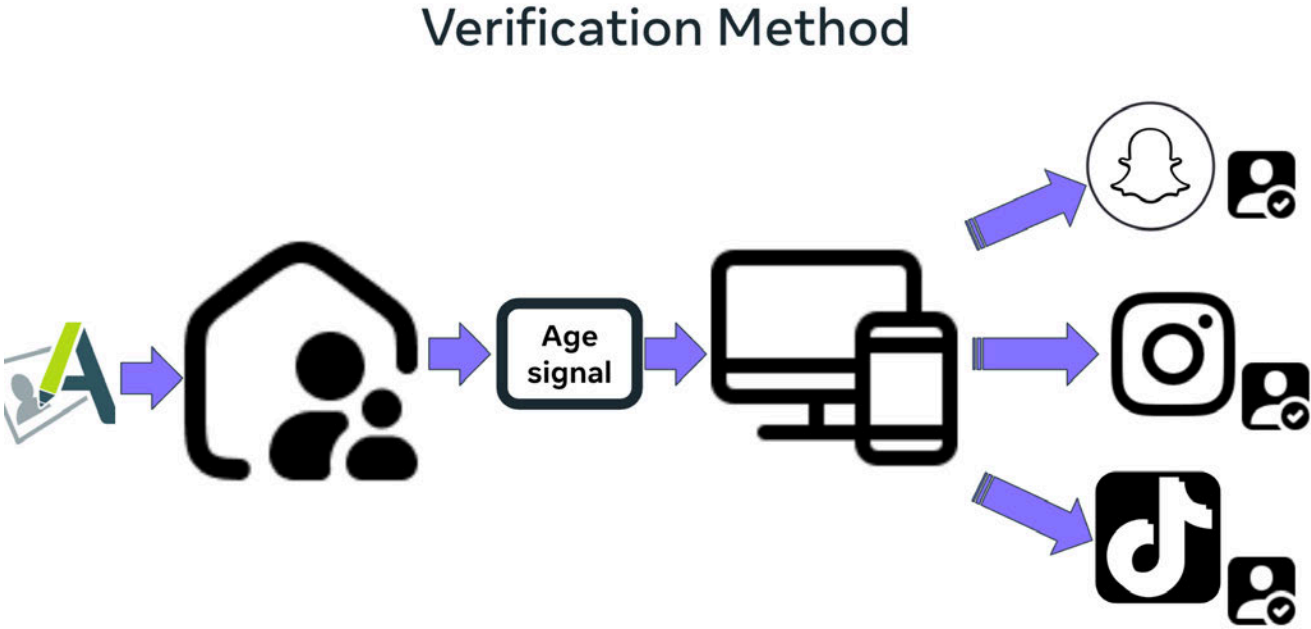
² Meta, ‘Limit sensitive content that you see on Instagram’ https://help.instagram.com/251027992727268?helpref=faq_content

We note that the Age Assurance Technology Trial intends to be – per the Project Plan – “an holistic project for Australia leading the world in building a thorough understanding of the effectiveness of age assurance as a practical tool for enhancing the protection of children online (and offline too)”. Given the recent announcements by several app store providers and regulatory developments in the US Federal Congress, as well as in Utah, California, and Singapore, we believe that this Trial best achieves this goal by outlining the ‘whole of ecosystem’ approach as the north star to which the entire tech stack should be working.

Our submission below is structured as much as possible in response to the questions outlined in the Practice Statement to provide an overview, technical information and responses to criticisms of the ‘whole of ecosystem’ approach.

Describe the system proposed

The proposed system is for age verification and parental approval at the OS or app store level. The image below outlines how this system would work.



As the diagram indicates, an app store would only share basic age signal information with individual third-party apps after a parent has given permission and the app store has confirmed the age of the young person. This basic information could include whether an account belongs to an adult or teen, or whether a teen is below a certain age – so that means describing the age within a range, rather than the precise age of that particular young person.

The app would not receive sensitive personal information like names of the parent or teen. The app could just be told the age range of the teen (eg, “under 16”) and whether their parent

approves the download. This helps ensure the teen's age is accurately reflected across all of the apps the parent approves, and helps individual apps build stronger parental supervision tools and more age-appropriate experiences for teens.

There are examples of app stores collecting parental consent and age information to provide some of their existing services, and so this can be extended via an API to provide age category information. For example, Meta is taking this approach in our own app store on Meta Quest headsets: apps that are for Mixed Ages (both users younger than 13 and users older than 13) can access our "Get Age Category API" to understand whether the app is being used by a preteen, teen, or adult user. The app is then able to use this information to tailor a more age-appropriate experience in their app or game and to properly protect young people's data.

Please describe how your system and practice statement are kept under continuous and regular review, including by your top management

In the context of the Australian Online Safety Amendment (Social Media Minimum Age) Act 2024 (the SMMA Act) and Australia's online safety regulatory requirements under the Online Safety Act 2022 (OSA) on digital platforms generally, regular review would occur to be to ensure age signals - from app stores as well as on social media and other platforms are subject to similar requirements under the SMMA Act and the OSA's Phase 2 Codes

With respect to Meta, we have a long-standing investment in promoting age assurance experiences and have built many tools and aspects of our content governance system based on the age signal we receive. For example, we add a warning label to some graphic or violent imagery so that people are aware it may be sensitive before they click through. We also restrict the ability for users under 18 to view such content.³

Age assurance components

There are three main components to Age Assurance:

- 1) Age Collection,
- 2) Age Verification, and
- 3) Age API (Operating System ↔ Application data sharing).

Each has options for technical implementation that balance the tradeoff between amount of data shared, user experience, and impact on overall age assurance.

In this document, we are providing a step by step walk through of this on the phone but the overall flow would be similar for a computer or other device, even though the specific technical details would differ from what we have outlined here.

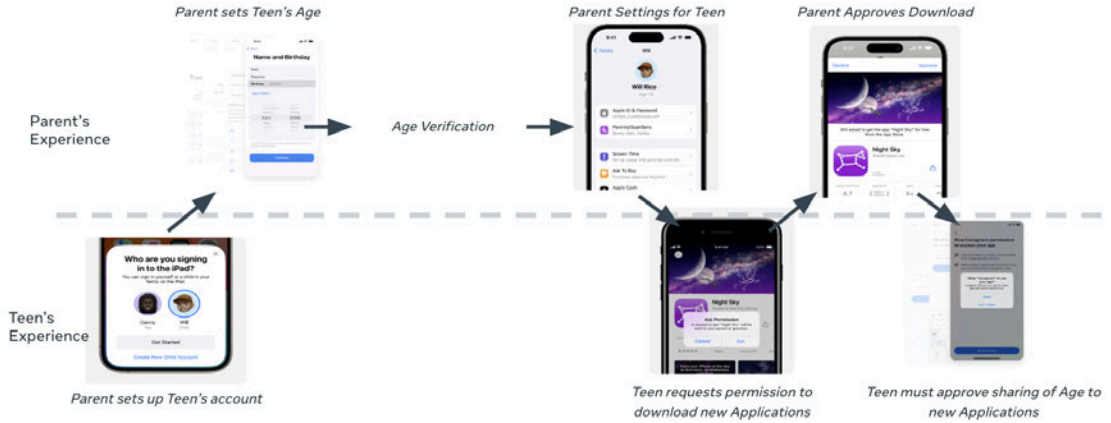
³ See Facebook Community Standards, Violent and graphic content:
<https://transparency.meta.com/en-gb/policies/community-standards/violent-graphic-content/>

Age verification: setting up age on a device

TECHNICAL WALKTHROUGH

A practical look

Age Verification and Parental Approval are closely coupled when setting up a new device.



The 'whole of ecosystem' approach leverages a 'golden moment' when a parent or guardian gives their child a device - at that moment parents are well placed to verify their child's age when setting up their phone and app stores can then apply that age to any apps young people want to download.

This solution makes it (1) easy on parents; (2) gives parents control; (3) and does so in a privacy-protective way - while also ensuring that teens are protected across the ecosystem of many, many apps. With this solution:

- It takes the burden off parents to verify age multiple times across multiple apps and for apps to collect potentially sensitive identifying information.
- Parents can ensure their teens are not accessing adult content or apps, or apps they just don't want their teens to use by approving app downloads and providing the relevant age signal.
- Where apps such as those provided by Meta offer age-appropriate features and settings, parents can help ensure their teens are placed in them
- Age verification at the level of an app store or OS with an app store also reduces barriers for new and smaller developers, making it easier for them to meet the expectations of parents and policymakers — providing a healthier competitive market.

Technical walkthrough: age verification

For age verification this utilizes a secondary source to increase confidence that a user's stated age is accurate. There are a number of options for the secondary source, and in practice it could be customized based on jurisdictional availability or best practices. For example:

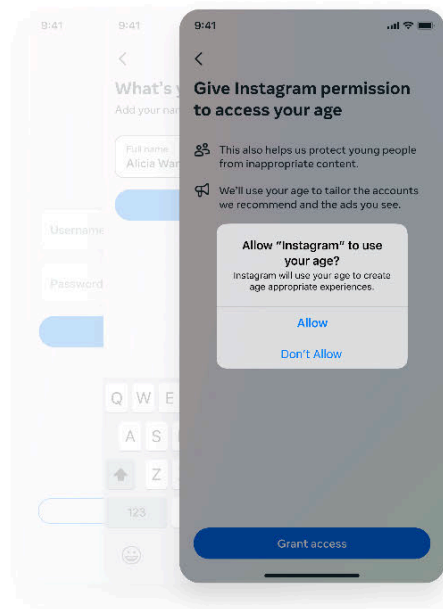
- *Parent-driven Age Verification.* If using Parental Approval or Supervision, the parent can supply the teen's date of birth.

- *Third Party Age Verification.* Operating Systems with app stores can interface with third party systems to securely verify a user’s stated age. This could include integration with an electronic ID if one is available.
- *Third Party Age Signals.* There are a number of third parties that use user-provided signals to estimate age. For example, Yoti provides Face-Based-Age-Prediction, which estimates a user’s age based on a “selfie.”

Age API: OS App Store <-> Application Data Sharing

The Age API (Operating System app store ↔ Application data sharing) provides the ability for the Operating System to give individual Applications access to age signals. The Operating System may choose to build user controls, similar to other operating system ↔ application data sharing.

There is optionality in how much data is shared, with sharing more granular data resulting in more age assurance capabilities.

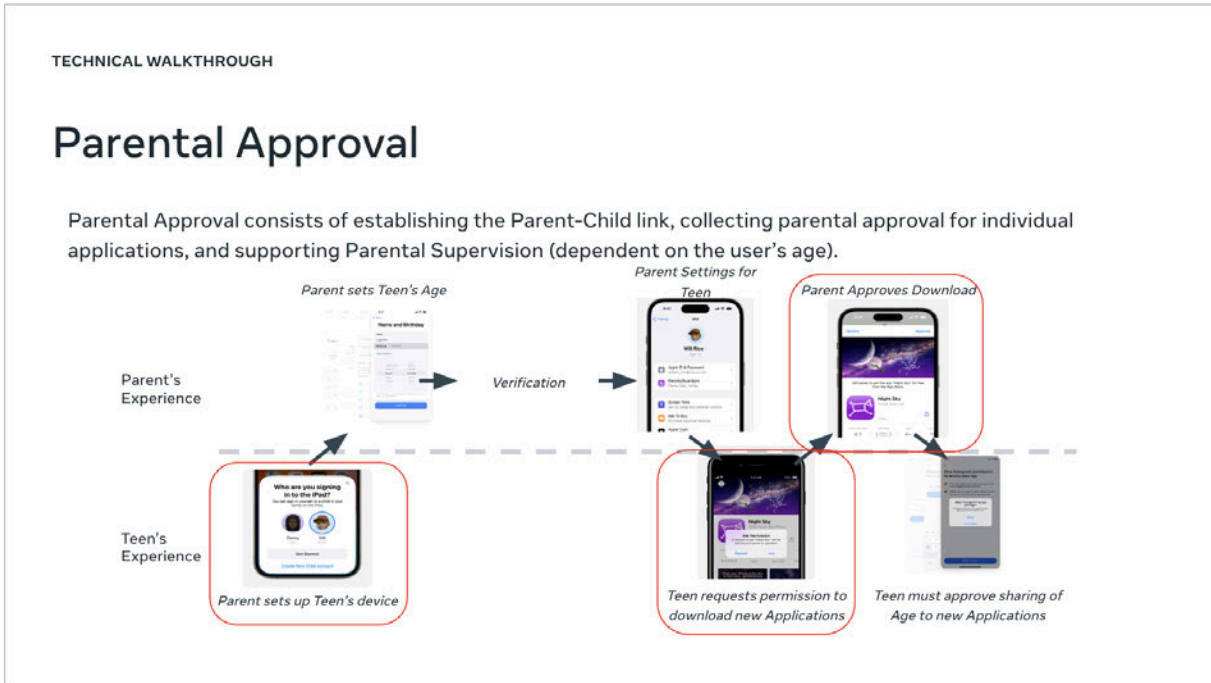


How these age signals are utilized once shared with the application can be varied based on the intended use case, ranging from completely disallowing access to an app, to applying more protective default settings, to gating specific user experiences.

For example, within the Facebook application:

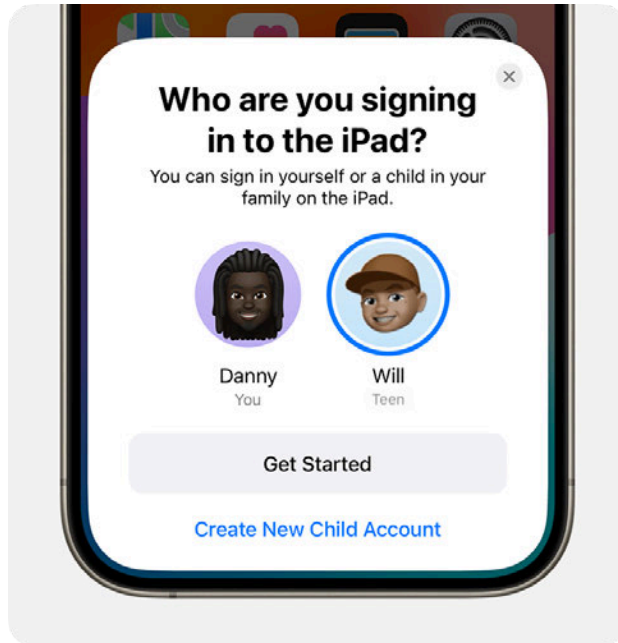
- “Checkpointing” a user for further age verification if the age signals provided by the OS disagree with other age signals
- Restricting access to age inappropriate content within features such as Feed or Reels.

Technical walkthrough: parental approval



Parent-Child Link

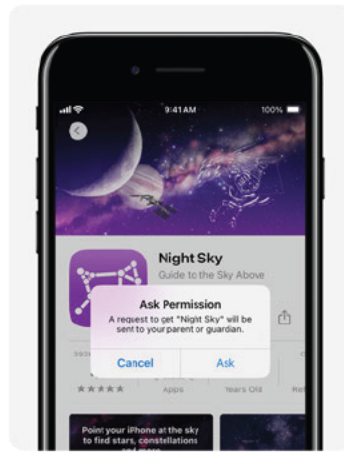
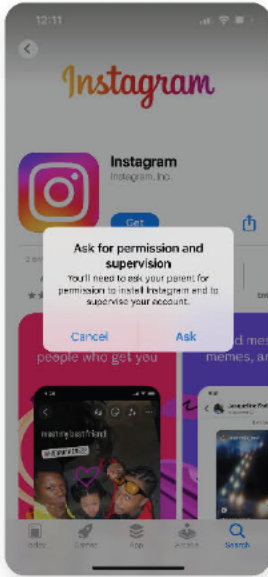
The Parent-Child Link is established by the parent when first setting up the teen's phone. This can also be done later on, for example, to support teens that already have devices when this feature is introduced, but requires access to both the parent and teen device to ensure safety of the teen. This link requires each device to have a unique identifier, but the identifiers are stored securely on each device and are never shared with an Application.



Parental approval of individual applications

The ability for parents to approve downloading individual applications already exists on many app stores today.

In addition to receiving a notification when a teen asks permission to download, the parent would also be able to subsequently revoke approval from within the Parent-Child Link controls.

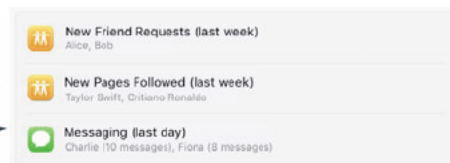


Parental supervision

To support Parental Supervision, the teen's device communicates with the app store Operating System via a predefined API. This API is extensible, allowing each Application to define which categories of data can be supervised, as well as the data which will be shared with the parent. For example, Facebook could provide information about new friend (connection) requests, new pages their teen has followed, and who they have messaged recently.

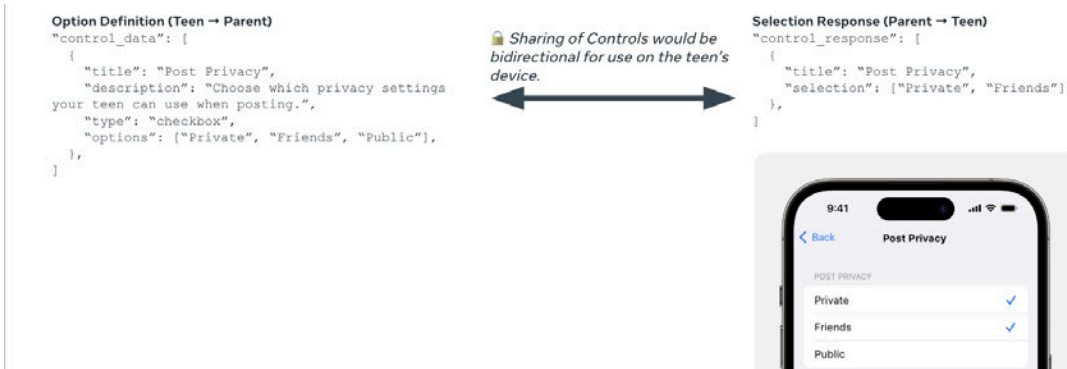
```
"supervision_data": [  
  {  
    "title": "New Friend Requests (last week)",  
    "icon": "",  
    "data": "Alice, Bob"  
  },  
  {  
    "title": "New Pages Followed (last week)",  
    "icon": "",  
    "data": "Taylor Swift, Cristiano Ronaldo"  
  },  
  {  
    "title": "Messaging (last day)",  
    "icon": "",  
    "data": "Charlie (10 messages), Fiona (8 messages)"  
  },  
]
```

Shared securely between the teen's and parent's device by the OS.

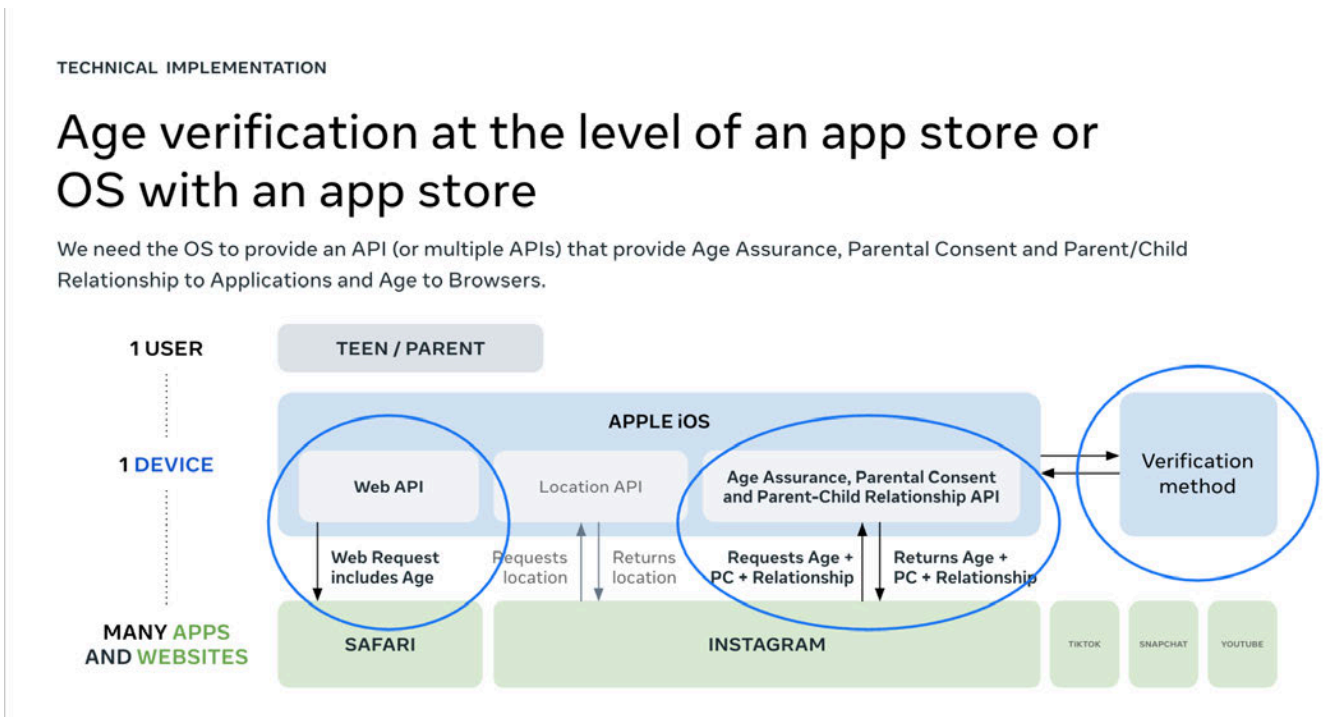


Parental Controls

This extensible approach could also support “Parental Controls” in the future, for example, allowing a parent to limit the reach of their teen’s posts.



This is how requiring express parental consent for teen users for all apps executed at OS/app store level can be achieved.



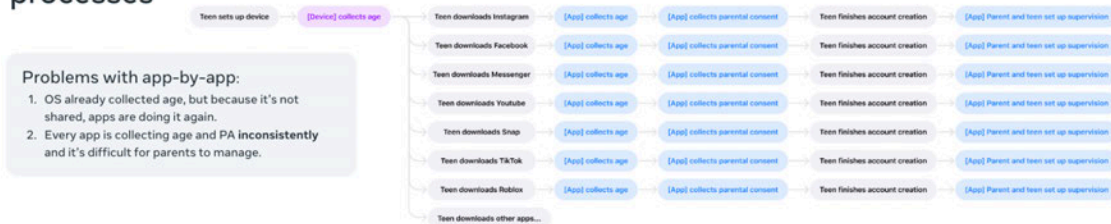
Privacy and data protection/ ease of use

Individual apps don't need your personal information from the app store – only some kind of age signal of the user and a confirmation of parental approval, if the person is under 16.

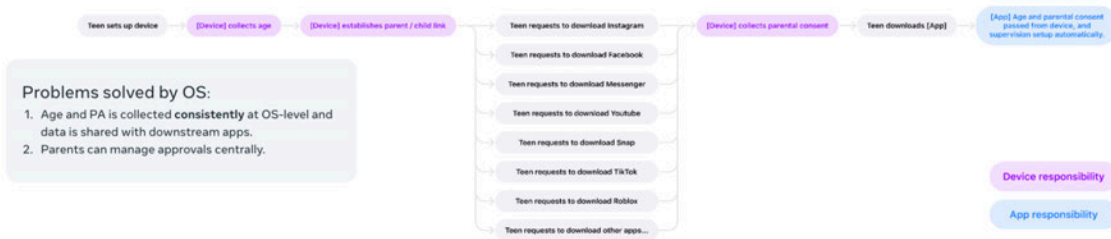
An easy way to accomplish this is through an API, a common way of sharing between apps.

CURRENT SITUATION

Current app-by-app experience is high-friction for parental approval processes



OS/App store experience is much simpler for parental approval processes



This approach is simpler and more secure as teens use multiple apps a week. Approval at the app level would mean over 40 different approval and age verification methods for parents to navigate. Busy parents don't have time for this. For example, instead of having to provide an ID to Roblox, Snapchat, TikTok, Instagram, Reddit, YouTube, and the plethora of other apps teens use, parents only need to provide an ID once to Apple or Android.

Some laws only apply to certain apps and websites. So to skirt protections put in place by apps implicated by these laws, teens can simply download less safe apps. The cost of compliance cannot be understated; small and emerging apps and platforms may not be able to comply with age assurance requirements.

Problems with app-by-app:

1. OS's with app stores already collected age, but because it's not shared, individual apps are doing it again.
2. Every app is collecting age and parental approval **inconsistently** and it's difficult for parents to manage.

Problems solved by OS's with app stores:

3. Age and parental approval is collected **consistently** at OS-level and data is shared with downstream apps.
4. Parents can manage approvals centrally.

Responding to concerns with respect to the ‘whole of ecosystem’ approach

There have been several concerns expressed with the proposed ‘whole of ecosystem’ approach. To assist the AATT, we have provided responses to these concerns to hopefully provide useful context as the AATT continues its work.

Specifically, these are:

- *Apps are shirking their responsibility:* App providers such as Meta are not shirking their responsibility by advocating for this approach. We will continue with the information available to ensure age appropriate experiences – our recent launch and expansion of Teen Accounts makes clear our commitment to built-in protections for teens and our support for parental involvement. Additionally, we recently started testing AI technology in the US that will proactively find accounts we suspect belong to teens, even if the account lists an adult birthday, and place them in Teen Account settings. Since rolling out Teen Accounts in September 2024, 97% of teens placed in Teen Accounts have stayed in the most strict settings. An app store/OS-level solution would be an important complement to these efforts and help ensure teens are safer not just on our apps but across all the apps they use.
- *Opt-in signal sharing:* By just sharing with developers who need the information to deliver age-appropriate experiences, and only sharing the minimum amount of data needed to provide an age signal, it reduces the risk of sensitive information being shared broadly.
- *Privacy:* Teens and parents already provide companies like Apple and Google with this information and these companies have already built systems for parental notification, review, and approval into their app stores. Meta’s investment in User Age Group APIs, which shares age category with app developers in the app store on Meta Quest is an example of how this can be achieved in a privacy-preserving way.
- *Verification method:* Parents continue to keep an eye on their teens' devices even after they’re set up - leveraging device-level parental supervision tools or connecting phones through things like Apple Family Sharing or Google Play Family Library for shared credit card purchases and location sharing.
- *Assumes familial relationships:* While we understand every family make-up is different, the benefit of this solution is that it encourages conversations between parents and/or guardians and young people about online safety and digital technology, which is generally agreed to be the best approach to keeping young people safe online.