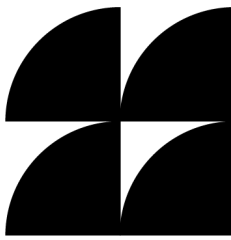
Knight Georgetown Institute

JULY 2026

Assigning Responsibility for Age Assurance:

Recommendations for Youth Online Safety

Amy Winecoff
Alissa Cooper
Knight-Georgetown Institute



About the Knight-Georgetown Institute

The Knight-Georgetown Institute (KGI) is dedicated to connecting independent research with technology policy and design. KGI serves as a central hub for the growing network of scholarship that seeks to shape how technology is used to produce, disseminate, and access information. KGI is designed to provide practical resources that policymakers, journalists, and private and public sector leaders can use to tackle information and technology issues in real time. Georgetown University and the Knight Foundation came together to launch the institute in 2024. Learn more about KGI at https://kgi.georgetown.edu.

Table of Contents

I. Introduction

As governments around the world look for ways to make online experiences safer for young people, age assurance – the process of determining whether a user meets a specified age threshold – has quickly become one of the most prominent regulatory tools. Legislators have proposed and enacted a growing number of laws that require digital services to estimate, verify, or otherwise determine a user's age. The use cases for these laws largely fall into two categories: (1) establishing safer defaults that provide tailored age-appropriate experiences for youth, and (2) blocking access to content, services, or accounts for users under a specific age.[1]

This rapid rise of age assurance has fueled debate about its potential benefits and drawbacks. Proponents portray age assurance as a necessary tool for addressing harms to youth, such as online grooming and sextortion,[2] excessive social media use,[3] and exposure to adult content,[4] while critics argue that existing approaches may be easily circumvented,[5] privacy-invasive,[6] or exclusionary to legitimate users who are legally entitled to access.[7]

Establishing a user's age and using that information to provide age-appropriate online experiences involves a series of related functions. These include assessing a user's age, communicating the resulting age information to the relevant service, and implementing the protections, defaults, or restrictions that correspond to the user's age signal. These functions can be carried out by different actors – such as device manufacturers, operating system (OS) providers, app store providers, dedicated age verification providers, and app developers – and implemented using a variety of technical architectures, with important implications for effectiveness, privacy, service availability, and resistance to circumvention.

Where laws require age assurance, determining which entities should be responsible for which functions requires making choices about policy goals and acceptable tradeoffs.[8] This brief evaluates those choices and offers concrete recommendations for the case where age assurance requirements are imposed to establish safer defaults for youth. Requiring safer defaults rather than denying access altogether may ease the transition to healthier patterns of online activity and create stronger norms or

[1] Age assurance can serve multiple purposes, including enabling age-appropriate experiences and safer defaults for youth, as well as restricting access to age-gated content or services. Different use cases may warrant different regulatory approaches. This brief focuses specifically on the use of age assurance to support safer defaults for youth online.
[2] Sandle et al., “Big Tech Firms Must Stop Young People Circulating Nude Images, Says UK PM Starmer”; O’Leary, *Why Roblox Is Being Sued by Nebraska’s Attorney General*.
[3] Twenge, “I Tried to Protect My Kids from the Internet. Here’s What Happened.”
[4] Twenge, “I Tried to Protect My Kids from the Internet. Here’s What Happened.”
[5] Editorial Board, “Teen Social Media Bans Are Destined to Fail”; Internet Matters and BMG Research, *The Online Safety Act*.
[6] Thomas, *Discord’s New Age Verification Is about to Spy on Every Message*.
[7] Williams, “‘I Can’t Believe This Is Happening’: iPhone Users Are Threatening to Defect to Android over New iOS Age Verification Push — and I’d Do the Same”; Thomas, *Discord’s New Age Verification Is about to Spy on Every Message*.
[8] Liu and Scheffler, “Adequately Tailoring Age Verification Regulations.”

incentives for compliance with age gates over time.[9] Approaches requiring safer defaults may also prove more legally defensible depending on the jurisdiction.

This brief treats age assurance as one tool among many for improving young people's online experiences, rather than as a standalone intervention intended to eliminate all underage access. From this perspective, the relevant question is not whether a particular age assurance system can prevent every instance of underage access, but whether it meaningfully reduces risks to youth while limiting negative impacts on privacy, service availability, competition, and openness.

Consistent with that objective, this brief examines the roles that app developers,[10] operating systems, and app stores can play in age assurance and evaluates the tradeoffs associated with different approaches. It argues that, regardless of how users' ages are assessed or communicated, app developers should retain primary legal responsibility for ensuring that the age information they rely on to apply age-appropriate settings satisfies applicable legal requirements. In contrast, any legal obligations placed on device intermediaries to conduct age assurance in support of safer defaults should focus on operating systems. These obligations should be narrowly tailored to facilitating privacy-preserving age signaling to app developers in a limited set of circumstances. For establishing safer defaults, legal mandates should not impose requirements on app stores to signal age information.

The brief offers five recommendations to help policymakers assign responsibility for different age assurance functions to the appropriate entities:

1. **Assign accountability for complying with youth safety requirements to app developers.** For safer defaults use cases, legal mandates should put the responsibility for meeting youth safety requirements – including the adoption or reliance on age assurance systems sufficient to meet those requirements – on the entities that are in a position to act on age information most directly: app developers.
2. **Focus device intermediary obligations on operating system providers.** Focusing on a single type of intermediary avoids overlapping or duplicative obligations, and operating systems already serve the general purpose of signaling user or device information to apps.
3. **Limit age assurance obligations on operating system providers to supplying robust privacy-preserving age signals to apps that request them.** Age signaling obligations imposed on operating systems should be limited to developing the capability to transmit a privacy-preserving age signal, only when necessary, and with technical privacy guarantees whenever feasible.

[9] This is consistent with the final report from the European Commission's special panel on child safety online, which recommends a developmentally appropriate approach, recognizing that as children mature, they require both protection from online harms and continued access to digital services. See Fegert and Melchior, *Child Safety Online: Protecting and Empowering Minors in a Digital World*.

[10] In this brief, "app developers" refers to commercial providers of mobile applications. It does not include applications developed and shared by hobbyists or open-source communities.

4. **Restrict age assurance requirements on operating system providers to mobile device operating systems only.** Targeting mobile environments focuses interventions on the contexts where youth are most likely to experience harm.
5. **Do not undermine competition in app distribution.** If policymakers impose age assurance obligations on app stores, those requirements should not assume that operating systems and app stores are controlled by the same company, nor should they create incentives that favor such arrangements.

The next two sections provide technical and policy background and describe the pitfalls associated with some approaches to imposing legal obligations for age assurance on device intermediaries. Section IV explains the rationale for each recommendation and the tradeoffs that inform them.

II. Emerging Regulatory Models

Age assurance is not a single technical intervention but a sequence of steps. First, a user's age must be **assessed** using one or more sources of information, such as a government-issued ID, a facial image, or parental attestation. The result of the assessment, whether an exact birthdate, an age, or a broader age category, must then be **signaled** to the app developer responsible for acting on it. Finally, the appropriate protections, defaults, or restrictions based on the user's age eligibility must be **enforced** (also known as **gatekeeping**).

Each of these steps can be implemented through a variety of technical architectures and assigned to different actors. For example, an app developer might perform all three steps. Alternatively, an operating system could assess a user's age during device setup and provide an age signal to apps through an application programming interface (API). A third-party age verification provider could instead perform age assessment and signal the result to the app. Or responsibilities could be divided among multiple actors in other ways. Which entity takes which step, as well as the technical architectures used to implement them, have important implications not only for the effectiveness of age assurance, but also for other properties such as privacy, service availability, and resistance to circumvention.

Some of the earliest adopted laws requiring age assurance, including the UK Online Safety Act of 2023,[11] the Australia Online Safety Amendment (Social Media Minimum Age) Act of 2024,[12] and addictive feeds laws passed in California[13] and New York in 2024,[14] place responsibility for age assurance on specific kinds of service providers, including social media services. Under these approaches, covered service providers are responsible for using a determination of users' ages to

[11] *Online Safety Act 2023*, 2023 c. 50.
[12] *Online Safety Amendment (Social Media Minimum Age) Act 2024*, No. 127, 2024.
[13] *Protecting Our Kids from Social Media Addiction Act*, 2024 Cal. Stat. ch. 321.
[14] *Stop Addictive Feeds Exploitation (SAFE) for Kids Act*, S.7694A.

either restrict access to the service or particular features, or to provide age-appropriate experiences based on a user's age.

Increasingly, legislators and regulators are exploring ways to shift the requirement to perform some steps in the age assurance process onto app stores, operating system providers, or device manufacturers (known as “device intermediaries” throughout this document). Some policymakers, child safety advocates, and industry leaders have argued that placing requirements for age assurance on app stores, operating system providers, or device manufacturers is desirable because these providers act as a “chokepoint” for exercising control over what youth can access online.[15] By this logic, imposing age assurance requirements on mobile app stores provides a more concentrated mechanism than requiring each app provider to conduct age assurance independently.[16]

In such proposals, operating system providers and app stores are required to carry out two distinct age assurance steps: **signaling** and **gatekeeping**. In the **signaling role**, the device intermediary (operating system or app store) is responsible for transmitting an age signal to app developers, who are then responsible for implementing the required age-modifications based on that signal. For example, California's Digital Age Assurance Act[17] requires operating system providers to collect a user's birthdate or age during account setup "for the purpose of providing a signal regarding the user's age bracket" and to make that signal available to app developers through a real-time API. It further requires developers to request the signal from an operating system provider or covered application store and "use that signal to comply with applicable law." The proposed Illinois HB 4140[18] and New York S.8102B[19] adopt largely similar structures, requiring the intermediary to collect age information and provide developers with a digital signal indicating the user's age category through an API.

In the **gatekeeping role**, the device intermediary restricts access to apps, purchases, or in-app purchases based on the user’s age and, for youth, parental consent. To date, this role has primarily been assigned to app stores. For example, the Texas App Store Accountability Act[20] requires app stores to establish users’ age categories when users create accounts and, for minors, to affiliate the minor’s account with a parent account and obtain parental consent.

---

[15] *Schoenbaum, Utah Becomes the First State to Pass Legislation Requiring App Stores to Verify Age; Lee, “Lee Introduces Bill to Protect Children Online, Hold App Stores Accountable.”*

[16] According to AppBrain, the Google Play Store hosts over 1.8 million apps. See AppBrain, “Android and Google Play Statistics.” According to Apple, the App Store hosts nearly 2 million apps. See Apple, *2025 App Store Transparency Report*.

[17] *Digital Age Assurance Act*, 2025 Cal. Stat. ch. 675.

[18] *Digital Age Assurance Act*, H.B. 4140, 104th Gen. Assemb. Illinois H.B. 4140 requires an operating system to collect users’ age or birthdate during account set up and provide an age category signal to app developers.

[19] *Device-Level Age Assurance*, S.8102B. New York's S.8102B requires a “covered manufacturer,” which includes a “manufacturer of an internet-enabled device, an operating system provider or an application store” to conduct age assurance when an internet-enabled device is activated.

[20] *App Store Accountability Act*, Tex. Bus. & Com. Code ch. 121 (S.B. 2420).

III. Pitfalls of Emerging Regulatory Models

In some scenarios, involving operating systems in age assurance can support the goals of age assurance while reducing privacy risks by limiting the entities that must collect and process age data. Age information configured by a user or parent during device setup and then shared with app developers in the least detailed form necessary can eliminate the need for each app to independently assess age eligibility. Notably, some operating system providers have already begun offering these capabilities voluntarily, without legal mandates.[21]

However, recognizing that operating systems can support age signaling is different from requiring all operating system providers to generate age signals and requiring app developers to rely on them. As legislative and regulatory proposals placing obligations on operating systems and app stores have proliferated, common pitfalls have emerged that risk undermining not only privacy goals but also other valuable characteristics of how online services are accessed today – including the openness of consumer computing environments, the general-purpose nature of personal devices, and the diversity of operating systems, browsers, and app stores available to users. Achieving age assurance through tighter platform control can come at the cost of users' ability to install software of their choice and of competition among device and software providers, entrenching the most closed ecosystems at the expense of competitive alternatives. Common pitfalls include:

Overbroad obligations. Some legislative proposals define covered entities so broadly that they extend beyond the existing mobile market duopoly. This risks sweeping in a much wider range of open- and closed-source operating system providers for desktop computers, gaming consoles, and other devices that present reduced risk profiles for safer defaults use cases, and that policymakers may not even intend to regulate. Overbroad obligations can also implicate open-source developers and communities,[22] who lack the corporate infrastructure of large technology companies and therefore are poorly positioned to comply with such requirements. The result is a compliance burden that poses risks to general-purpose computing and open-source software distribution.[23]

Scope and mission creep. Some legislative proposals may inadvertently allow age assurance systems to expand beyond their intended scope or purpose. Scope creep can occur when legal requirements do not clearly limit the information that age assurance systems may collect, process, retain, or transmit, increasing privacy risks without improving age assurance outcomes. A related concern is mission creep, in which age assurance systems developed for the narrow purpose of establishing age eligibility are gradually repurposed for unrelated functions. This can occur when legislation does not clearly limit the permissible uses of age assurance data or infrastructure, enabling

[21] Apple. “Apple Expands Tools to Help Parents Protect Kids and Teens Online.”
[22] Rescorla, *How Not to Mandate Device-Based Age Assurance*.
[23] Rescorla, *How Not to Mandate Device-Based Age Assurance*; “California Age Verification Law Linux: What AB 1043 Means for Open Source.”

their use for purposes such as identity verification, advertising, profiling, fraud detection, or other auxiliary functions beyond establishing age to determine which system defaults apply.

Misaligned and overlapping obligations. Some proposals treat distinct actors in the technology stack as though they all perform the same role. New York's S.8102A,[24] and Illinois' H.B. 5511,[25] for example, group device manufacturers, operating system providers, and app stores into a single "covered manufacturer" category and impose identical obligations on each. In practice, these actors perform different technical roles and frequently represent different organizations. A single device may be manufactured by one company, run an operating system developed by another, and distribute applications through an app store operated by a third. By applying the same requirements to each, such policies create uncertainty about which entity is responsible for particular age assurance functions, potentially complicate coordination among independent entities, and raise the possibility for duplicative or inconsistent age signaling, even within the same user interaction.

Dependency on mobile ecosystem concentration. Many proposals that implicate operating system providers and app stores are motivated by the unusually concentrated structure of today's mobile ecosystem.[26] Because Apple and Google currently exercise substantial control over mobile operating systems and app distribution,[27] policymakers may view these actors as efficient intervention points through which obligations can be implemented by a relatively small number of companies. However, this efficiency is a product of current market conditions rather than an inherent feature of age assurance. The concentration of the mobile ecosystem may make certain approaches easier to deploy, but effective age assurance should not depend on maintaining that concentration.

Weak privacy design. Many proposals require age information to be disclosed to apps or websites regardless of whether those services have a meaningful need for the information or any obligation to act on it, unnecessarily expanding the distribution of sensitive data. Some proposals fail to establish robust privacy protections governing the collection, storage, transmission, and retention of age-related information, increasing the likelihood that such data will be exposed, retained, or misused. Some proposals focus on signaling age ranges, rather than specific age or birthdate information; while the practice of sharing age categories is generally less risky than sharing exact age or birthdate information, signaling age ranges still creates privacy risks. For example, a user must still share more granular information to establish their age category in the first place, which if handled improperly, could lead to privacy-related harms.

The next section provides five recommendations for avoiding these pitfalls in cases where policymakers choose to adopt operating system or app store obligations in service of applying safer defaults for youth.

---

[24] *Device-Level Age Assurance*, S.8102B

[25] *Children's Social Media Safety Act*, H.B. 5511, 104th Gen. Assemb.

[26] Sustained lobbying from service providers, most notably Meta, bears responsibility for policymaker interest in these approaches. See Reader, "How Mark Zuckerberg Is Flipping the Script on Kids' Safety Online."

[27] Competition and Markets Authority, *CMA Confirms Apple and Google Have Strategic Market Status in Mobile Platforms*.

IV. Policy Recommendations for OS- and App Store-Based Age Assurance

The pitfalls described above suggest that any role assigned to device intermediaries in support of safer defaults should be carefully limited and designed to preserve accountability, privacy, competition, and openness. The five recommendations below set out a framework for identifying when operating system-based age assurance is justified in support of safer defaults, how such requirements should be constrained, and where policymakers should avoid relying on operating systems or app stores.

1. **Assign accountability for complying with youth safety requirements to app developers.** For safer defaults use cases, legal mandates should put the responsibility for meeting youth safety requirements – including the adoption or reliance on age assurance systems sufficient to meet those requirements – on the entities that are in a position to act on age information most directly: app developers.

The circumstances under which youth experience harm from using social media, AI chatbots, and other online services are inherently created and facilitated by app developers themselves.[28] Many of the most important interventions for mitigating those harms, including changes to product design, recommendation systems, notification structures, and content moderation, can only be implemented by the app developers themselves since they control the product functionality. As a result, app developers are the actors best positioned to modify those design decisions in ways that better support the well-being of youth, and legal frameworks should preserve clear responsibility for them to do so.

App developers should be able to choose whether and to what extent they rely on third parties, including operating system providers, age verification providers, or others, to fulfill age-related requirements prescribed by law. This is consistent with how accountability is assigned in other industries with complex supply chains. A restaurant remains responsible for serving safe food even though it relies on farmers, distributors, and other suppliers. It manages those dependencies through vendor selection, contracts, audits, insurance, and other risk-management procedures because – as the provider of the product to the consumer — it remains responsible for ensuring safety. App developers are similarly well positioned to select age assurance providers, or implement age assurance steps themselves, to allow them to meet their youth safety obligations. Prescribing a single source of age information risks calcifying particular technical architectures, discouraging innovation in age assurance that could improve accuracy, privacy, accessibility, and resistance to circumvention, and weakening incentives for providers to adopt better approaches as they emerge.

[28] Children and Screens: Institute of Digital Media and Child Development et al., “Comments to the Office of the New York State Attorney General on the Proposed Rules for the SAFE for Kids Act”; Costello et al., “Algorithms, Addiction, and Adolescent Mental Health.”

In contrast to app developers, app stores and operating systems are poorly positioned to make nuanced decisions about how specific apps should function for different users. Because they have limited visibility into the features, risks, and contexts of use for individual apps and services, policies that rely on them as intermediaries of the age assurance process can be both over- and under-inclusive. For example, youth and their parents may have good reasons for wanting to retain access to certain features within an app, such as private messaging among family, or tools used for schoolwork, while having other features blocked or turned off by default. App stores and operating systems do not have the granular ability to provide these tailored experiences based on age information – the only controls they can offer are to either block or allow apps in their entirety. In other words, operating systems and app stores are poorly positioned to enforce feature-level age-appropriate protections.

One objection to holding app developers responsible for meeting age-related requirements is that it could place the burden of conducting age assurance on all app developers, including small providers with limited resources, expanding the overall privacy risk surface. However, if the goal of a youth online safety policy is to meaningfully reduce harmful online experiences rather than eliminate every instance of underage access, legal obligations to protect youth safety could be limited to services that reach a sufficiently large number of users or pose the greatest risks to youth. Limiting coverage both reduces unnecessary collection of age-related information and focuses regulatory efforts where they are likely to have the greatest impact.

2. **Focus device intermediary obligations on operating system providers.** If device intermediaries are assigned legal obligations to conduct age assurance in support of safer defaults, the simplest approach is to focus those obligations on operating system providers. Focusing on a single type of intermediary avoids overlapping or duplicative obligations, and operating systems already serve the general purpose of signaling user or device information to apps.

As noted above, some legislative proposals place legal obligations to support or conduct age assurance on multiple different kinds of device intermediaries. This can unnecessarily increase the number of parties required to collect, store, or transmit age information, and it could create complications or inconsistencies in the age information that gets signalled to apps. Focusing on a single type of intermediary, if intermediaries are going to be the subject of legal obligations, potentially limits age information exposure and simplifies compliance.

If device intermediaries are being subject to legal obligations requiring them to signal age information to apps, operating system providers are the most straightforward target for those obligations. Operating systems already expose APIs that allow apps to learn information about the user or device in real time, and their general purpose is to create an environment with the features needed for apps to run. Every consumer-facing app already makes use of the functionality provided by the operating system.

App stores, which are just apps themselves running on the operating system (or at times in a browser), perform a more narrow function: facilitating the discovery, distribution, and installation of apps, and supporting app monetization. Apps can be downloaded and installed without going through an app store (with apps running on Apple iOS and iPadOS devices being a prominent exception). Because of this, placing legal obligations on app stores to signal age information, and on apps to consume that information, could create new dependencies between apps and app stores that do not currently exist. Such obligations overload the purpose of app stores with additional functionality that could unnecessarily serve to further entrench native app stores as gatekeepers for app distribution (see recommendation #5 below).

App stores have become a common target for enforcement of blocking mandates. But for policies aimed at creating safer default experiences for youth, there is a better choice of device intermediary to involve – the operating system – that does not have these drawbacks.

3. **Limit age assurance obligations on operating system providers to supplying robust privacy-preserving age signals to apps that request them.** Age signaling obligations imposed on operating systems should be limited to developing the capability to transmit a privacy-preserving age signal, only when necessary, and with technical privacy guarantees whenever feasible.

Consistent with the previous recommendation, age assurance obligations placed on operating system providers should be focused on facilitating the availability of OS-provided age signals as one option that app developers may leverage to meet their own legal obligations. To minimize privacy risks, OS-level age assurance policies should limit who receives age-related information, when it is transmitted, and how much information is shared. While OS-based approaches may reduce privacy concerns relative to alternatives, they still involve the creation, storage, transmission, and sharing of age-related information, which makes the inclusion of robust privacy safeguards paramount.

Privacy risks can be reduced by limiting the precision of the information that is disclosed. Transmitting age information in broad categories (e.g., under 13, 13–17, 18+) can reduce privacy risks relative to approaches that rely on more granular age data, although even coarse age categories may themselves reveal sensitive information. Age ranges still contribute to user or device fingerprinting, can reveal information about the user's birthdate or birth year when they cross an age range boundary, and may involve the collection of more specific age or birthdate information to determine the range to be signaled.

Another important safeguard is limiting the obligation on operating system providers to disclosing age signals to apps that have a legal requirement to act on that information. Broad sharing of age signals across the digital ecosystem increases the likelihood that information about users' identities or online activities will become accessible to actors beyond those directly involved in the age assurance process. Existing research shows that apps targeting teenagers often collect especially large amounts

of data,[29] underscoring both the commercial value of information about teens and the possibility that such systems may become attractive targets for adversarial actors. App store review processes are also not failsafe; malicious apps have appeared on both major app stores,[30] and research has shown that app developers often collect and use data in ways not disclosed to users in their privacy policies.[31] Restricting the operating system disclosure requirement to services that are legally required to use age signals aims to reduce the number of entities that can collect, retain, infer, or misuse sensitive information about users and their online activities.

Persistent or automatic transmission creates additional opportunities to link age-related information with other data about users and their activities. Even age category data can become highly revealing when combined with browsing histories, location data, device identifiers, or other datasets. Restricting age-signal transmission to specific, on-demand requests therefore helps limit unnecessary data sharing and reduces the risk that age assurance systems in practice become tools for behavioral tracking, commercial profiling, or government surveillance.[32]

Requirements that operating system providers adopt governance and data management practices that limit the collection, use, retention, and disclosure of age-related information are non-negotiable. However, because these practices are difficult for users and external stakeholders to independently verify,[33] governance requirements alone provide only limited assurance that providers are handling users' information as intended. Where commercially feasible, operating system-based age assurance obligations should require technical mechanisms that provide verifiable privacy guarantees rather than relying solely on governance controls.

For example, cryptographic techniques such as zero-knowledge proofs and selective disclosure can ensure that only the minimum information necessary for a given purpose is disclosed, making compliance with data minimization and purpose limitation requirements technically enforceable rather than dependent solely on app developer practices. As approaches based on these techniques mature and become more commercially available,[34] legal provisions should require their adoption, where the system architectures involved are suitable for these techniques to be deployed.

---

[29] Mariani et al., “Analyzing Privacy Implications of Mobile Apps Data Collection across Age Groups.”

[30] Furnell, *Literature Review on Security and Privacy Policies in Apps and App Stores*.

[31] Hayes et al., “An Effective Approach to Mobile Device Management.”

[32] See Rescorla et al., *Age Assurance Online*, p. 28.

[33] Independent oversight is a critical component of any age assurance policy. Meaningful oversight requires that independent evaluators have sufficient access to the underlying systems, processes, and relevant data to assess whether covered entities—including operating system providers and app developers—are meeting their obligations. Such oversight is essential for verifying claims about the effectiveness, privacy, security, and accessibility of age assurance systems, rather than relying solely on providers' own representations. We discuss recommendations for independent oversight and evaluation in greater detail in Winecoff and Cooper, *Age Assurance Rules: An Implementation Guide*.

[34] Such approaches are already beginning to be deployed (See e.g., *Linarducci, “Bringing Secure Digital Identity and Payment Tools to More People”; European Commission, “The EU Approach to Age Verification.”)*

4. **Restrict age assurance requirements on operating system providers to mobile device operating systems only.**

Because the purpose of age assurance should be to reduce, rather than entirely eliminate, harms to youth online, policies focused on creating safer defaults should prioritize the technologies and contexts where those harms are most likely to arise: mobile apps.[35] Smartphone usage is widespread, with 95% of U.S. teens reporting having access to one.[36] In the United Kingdom, 90% of parents of youth ages 13 to 17 report that their child uses a mobile phone to access the internet, compared with 59% who report that their child uses a laptop.[37] These findings suggest that smartphones have become the primary device through which adolescents access online services.[38]

Many of the harmful design features safer defaults policies seek to limit — nighttime notifications, infinite scroll, and engagement-based feeds[39] — are most fully realized in mobile environments. While these features are sometimes available on desktop websites, smartphones combine them in powerful ways with device functionality like push notifications, lock-screen alerts, and device portability, creating opportunities for continuous engagement throughout the day. This is consistent with findings that nearly half of U.S. teens report being online "almost constantly,"[40] often receive hundreds of smartphone notifications each day, and frequently check their phones throughout both the day and night.[41] Accordingly, limiting age assurance requirements to mobile environments is likely to capture a substantial share of the user interactions that such policies are designed to modify.

This recommendation is not meant to minimize the potential for harm arising from youth access to websites or desktop experiences. Rather, it focuses mandatory age assurance – a complicated intervention involving many tradeoffs – on the contexts where it is likely to yield the greatest aggregate benefits.

Mobile devices are also the environment in which OS-based age assurance requirements are most practical to implement and enforce. Most iOS and Android devices operate as relatively closed systems in which users have limited ability to modify the software running on their devices. Users typically obtain applications through native app stores and less frequently sideload software or jailbreak their devices. As a result, the mobile ecosystem provides comparatively strong defenses against circumvention, making mobile device-based age assurance more effective.

---

[35] For a discussion of age assurance implementations and considerations for web browsers, see p. 41-44 and 99-102 in Rescorla et al., *Age Assurance Online*.
[36] Faverio and Sidoti, "Teens, Social Media and Technology 2024."
[37] Ofcom, *Children and Parents Media Use and Attitudes Report*.
[38] Industry sources of data also suggest a shift towards mobile. In July of 2026, Similarweb analytics reported that 65% of traffic comes from mobile devices. See Similarweb, "Mobile vs. Desktop Traffic Market Share [June 2026]." SensorTower reports that in 2024 users spent almost 2.4 trillion hours on social media apps. See SensorTower, "State of Mobile 2025."
[39] Ebster et al., "Taming the Endless Scroll?"; Nagata et al., "Smartphone Use on School Nights in the Adolescent Brain Cognitive Development Study"; Allen et al., *Better Feeds*; Costello et al., "Algorithms, Addiction, and Adolescent Mental Health"; American Psychological Association, *Potential Risks of Content, Features, and Functions*; Garrett et al., "Links Between Objectively-Measured Hourly Smartphone Use and Adolescent Wake Events Across Two Weeks."
[40] Faverio and Sidoti, "Teens, Social Media and Technology 2024."
[41] Common Sense Media, *Constant Companion*.

Desktop operating systems function very differently. Users can install software from a wide variety of sources, modify system behavior, and in some cases exercise complete control over the operating system itself.[42] At the most open end of the spectrum, users may run open-source operating systems such as Linux, where all software on the device, including the operating system, can be freely modified. These characteristics create numerous opportunities to circumvent age assurance or interfere with the signaling of age-related information. Achieving a degree of resistance to circumvention on desktop systems comparable to that of mobile devices would likely require significant restrictions on the software users can run on desktop and may be infeasible for many already-deployed systems. These concerns are especially relevant for software engineering and enterprise environments where use of alternative (often open-source) operating systems is widespread.

Applying age assurance requirements to operating system providers broadly construed also risks sweeping in actors that policymakers may not intend to regulate. Policymakers may intend these requirements to apply primarily to large commercial firms with substantial compliance infrastructure, such as Google, Apple, or Microsoft. However, open-source operating systems, including popular Linux distributions, are often developed by decentralized communities that lack centralized governance structures, user-tracking mechanisms, or the resources necessary to implement and maintain compliance systems.[43] Depending on how covered entities are defined,[44] these requirements could create legal uncertainty or liability risks for maintainers and contributors who are not realistically capable of complying with age assurance obligations.[45]

5. **Do not undermine competition in app distribution.** If policymakers impose age assurance obligations on app stores, those requirements should not assume that operating systems and app stores are controlled by the same company, nor should they create incentives that favor such arrangements.

Beyond concerns about app stores being a suboptimal choice for mandatory age signaling to apps, app store-focused approaches can also have unintended consequences for competition if they are designed in ways that assume the current market structure. Mobile app distribution is currently dominated by Apple and Google, whose control over both app stores and operating systems has historically limited competition.[46] Apple prohibits third-party app stores on iOS in most jurisdictions,

[42] Rescorla et al., *Age Assurance Online*.

[43] "California Age Verification Law Linux: What AB 1043 Means for Open Source."

[44] California's A.B. 1856 would amend the Digital Age Assurance Act to exempt open-source operating system developers. Although exempting open-source operating system distributions would reduce the burden on open-source communities, it would not resolve other technical challenges associated with implementing age assurance in desktop environments. See *Age Verification Signals: Software Applications and Online Services*, A.B. 1856.

[45] Notably, overly broad operating system provisions could also sweep in gaming consoles, smart TVs, and other connected devices that are not central to the harms policymakers are attempting to address. Limiting age assurance obligations to mobile operating systems would help avoid this kind of over-inclusion as well.

[46] United States. Congress. House. Committee on the Judiciary. Subcommittee on Antitrust, Commercial, and Administrative Law, *Investigation of Competition in Digital Markets: Majority Staff Report and Recommendations*; Competition and Markets Authority, *CMA Confirms Apple and Google Have Strategic Market Status in Mobile Platforms*.

while Google allows alternative distribution in principle but imposes enough friction to constrain its widespread use.

Regulatory and legal efforts are beginning to open app store provision to more competition. The EU Digital Markets Act,[47] the Japan Mobile Software Competition Act Guidelines,[48] and the remedies resulting from Epic Games lawsuits[49] require Apple and Google to open their platforms to alternative app stores and put additional guardrails in place to create a more level playing field for alternative app distribution.

Alternative app stores may perform a similar function to native app stores provided by Apple and Google, but they generally do not exist on equal footing with the native app stores. They do not typically arrive pre-installed on a user's device. Operating system providers may choose not to share their user account frameworks with alternative app stores, and may indeed have competitive incentives not to do so.

Laws that assume that a device will only have a single app store, or that the operating system and the app store will always be provided by the same vendor on a device, risk disadvantaging emerging app store competitors. For example, some proposals (e.g., in New York[50] and Michigan[51]) put age-assurance obligations on app stores at device setup, but alternative app stores may not yet be installed at device setup. California's Digital Age Assurance Act[52] requires operating system providers to collect age information during account creation and expose age bracket information to app stores. If alternative app stores use their own user account frameworks, tying the age information to the operating system's account framework could create additional friction for the user.

Establishing obligations on app stores that only Apple and Google can meet risks reinforcing the two companies' existing market power. If policymakers decide to pursue app store age assurance requirements, such proposals need to be carefully crafted. Obligations on app stores should not assume that app stores are pre-installed on mobile devices, that they have access to the operating system's user account infrastructure, that they have access to operating system APIs that any other third-party apps would not have, or that they are otherwise integrated in any way with the operating system or the device manufacturer.

[47] Regulation (EU) 2022/1925 (Digital Markets Act), OJ L 265, 12.10.2022.
[48] Japan Fair Trade Commission, *Mobile Software Competition Act Guidelines*.
[49] *Epic Games, Inc. v. Apple Inc.*, No. 25-2935.; *Epic Games, Inc & Anor v Google LLC & Ors*, NSD190/2021; *Epic Games, Inc. v. Google LLC*, No. 24-6256.
[50] *Device-Level Age Assurance*, S.8102B.
[51] *Digital Age Assurance Act*, H.B. 4429
[52] *Digital Age Assurance Act*, 2025 Cal. Stat. ch. 675.

V. Conclusion

Age assurance can play a role in supporting safer online experiences for young people, but only when implemented in ways that are responsive to the harms being addressed and that appropriately balance the benefits of age assurance against the costs to privacy, service availability, competition, and openness. As policymakers continue to explore age assurance mandates, new requirements should ensure that responsibility for complying with youth safety obligations remains with app developers, as they are the actors best positioned to prevent harm. This approach runs counter to some of the prevailing legislative proposals, which would place the onus for age-gating on app stores and thus allow app developers to avoid having to make design decisions that better protect their young users.

Obligations on device intermediaries should focus on operating system providers, whose role should be narrowly limited to transmitting privacy-preserving age signals to services with a legal obligation to act on them when necessary for compliance. Policies that extend beyond this limited role risk creating significant costs for privacy, competition, and open technology ecosystems without meaningfully improving protections for youth.

Bibliography

Age Verification Signals: Software Applications and Online Services. A.B. 1856, 2025–2026 Reg. Sess. California Legislature. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB1856

Allen, Jeff, Zander Arnao, Alissa Cooper, Motahhare Eslami, Nadine Farid Johnson, and Ravi Iyer. *Better Feeds: Algorithms That Put People First*. Knight-Georgetown Institute, 2025. https://kgi.georgetown.edu/research-and-commentary/better-feeds/.

American Psychological Association. *Potential Risks of Content, Features, and Functions: The Science of How Social Media Affects Youth*. American Psychological Association, 2024. https://www.apa.org/topics/social-media-internet/youth-social-media-2024.

Aneesha. "California Age Verification Law Linux: What AB 1043 Means for Open Source." *LinuxTeck*, March 10, 2025. https://www.linuxteck.com/california-age-verification-law-linux/.

App Store Accountability Act. Tex. Bus. & Com. Code ch. 121 (2025) (S.B. 2420). https://capitol.texas.gov/tlodocs/89R/billtext/html/SB02420F.htm

AppBrain. "Android and Google Play Statistics." May 31, 2026. https://www.appbrain.com/stats.

Apple. *2025 App Store Transparency Report.* Cupertino, CA: Apple, 2025. https://www.apple.com/legal/app-store/transparency/2025/

Apple. "Apple Expands Tools to Help Parents Protect Kids and Teens Online." *Apple Newsroom*, June 11, 2025. https://www.apple.com/newsroom/2025/06/apple-expands-tools-to-help-parents-protect-kids-and-teens-online/.

Children and Screens: Institute of Digital Media and Child Development, The Center for Countering Digital Hate, and ParentsTogether. "Comments to the Office of the New York State Attorney General on the Proposed Rules for the SAFE for Kids Act." December 2025. https://www.childrenandscreens.org/newsroom/news/children-and-screens-submits-expert-comments-on-safe-for-kids-act-proposed-rules/.

Children's Social Media Safety Act. H.B. 5511, 104th Gen. Assemb. Illinois General Assembly. https://www.ilga.gov/Legislation/BillStatus/FullText?DocName=10400HB5511eng&DocNum=5511&DocTypeID=HB&GAID=18&LegDocId=208832&LegID=167486&Session=&SessionID=114&SpecSess=.

Common Sense Media. *Constant Companion: A Week in the Life of a Young Person's Smartphone Use*. 2023. https://www.commonsensemedia.org/research/constant-companion-a-week-in-the-life-of-a-young-persons-smartphone-use.

Competition and Markets Authority. *CMA Confirms Apple and Google Have Strategic Market Status in Mobile Platforms*. October 22, 2026.

https://www.gov.uk/government/news/cma-confirms-apple-and-google-have-strategic-market-status-in-mobile-platforms.

Costello, Nancy, Rebecca Sutton, Madeline Jones, et al. "Algorithms, Addiction, and Adolescent Mental Health: An Interdisciplinary Study to Inform State-Level Policy Action to Protect Youth from the Dangers of Social Media." *American Journal of Law & Medicine* 49, nos. 2–3 (2023): 135–72. https://doi.org/10.1017/amj.2023.25.

Device-Level Age Assurance. S.8102B, 2025–2026 Reg. Sess. New York State Senate. https://www.nysenate.gov/legislation/bills/2025/S8102/amendment/B.

Digital Age Assurance Act. 2025 Cal. Stat. ch. 675 (A.B. 1043). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB1043.

Digital Age Assurance Act. H.B. 4140, 104th Gen. Assemb. Illinois General Assembly. https://www.ilga.gov/documents/legislation/104/HB/PDF/10400HB4140.pdf

Digital Age Assurance Act. H.B. 4429, 2025–2026 Reg. Sess. Michigan Legislature. https://legislature.mi.gov/documents/2025-2026/billintroduced/House/htm/2025-HIB-4429.htm

European Union. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). OJ L 265, 12.10.2022, 1–66. https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng.

Ebster, Marlene, Michael Lauerer, Eckhard Nagel, and Sebastian Schmidt. "Taming the Endless Scroll? Short-Form Videos, Digital Routines and Neurocognitive Outcomes in Youth: A Systematic Literature Review." *European Child & Adolescent Psychiatry*, ahead of print, June 13, 2026. https://doi.org/10.1007/s00787-026-03083-7.

Editorial Board. "Teen Social Media Bans Are Destined to Fail." *The Washington Post*, March 21, 2026. https://www.washingtonpost.com/opinions/2026/03/21/social-media-social-media-bans-australia-indonesia/.

Epic Games, Inc & Anor v Google LLC & Ors. NSD190/2021. Federal Court of Australia, filed March 8, 2021. https://www.fedcourt.gov.au/services/access-to-files-and-transcripts/cases-of-interest.

Epic Games, Inc. v. Google LLC, No. 24-6256 (9th Cir. July 31, 2025), https://cdn.ca9.uscourts.gov/datastore/opinions/2025/07/31/24-6256.pdf

Epic Games, Inc. v. Apple Inc., No. 25-2935 (9th Cir. Dec. 11, 2025). https://cdn.ca9.uscourts.gov/datastore/opinions/2025/12/11/25-2935.pdf

European Commission. "The EU Approach to Age Verification." May 13, 2026. https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification.

Faverio, Michelle, and Olivia Sidoti. "Teens, Social Media and Technology 2024." Teens & Tech. *Pew Research Center*, December 12, 2024. https://www.pewresearch.org/internet/2024/12/12/teens-social-media-and-technology-2024/.

Fegert, Jörg M., and Maria Melchior. *Child Safety Online: Protecting and Empowering Minors in a Digital World*. European Commission, 2026. https://commission.europa.eu/document/download/d833504d-5ec3-4fac-945f-38e7d0bd5326_en?filename=Special-panel-report.pdf.

Furnell, Steven. *Literature Review on Security and Privacy Policies in Apps and App Stores*. Department for Digital, Culture, Media & Sport, 2022. https://www.gov.uk/government/consultations/app-security-and-privacy-interventions/literature-review-on-security-and-privacy-policies-in-apps-and-app-stores.

Garrett, Shedrick L., Kaitlyn Burnell, Emma L. Armstrong-Carter, Benjamin W. Nelson, Mitchell J. Prinstein, and Eva H. Telzer. "Links Between Objectively-Measured Hourly Smartphone Use and Adolescent Wake Events Across Two Weeks." *Journal of Clinical Child & Adolescent Psychology* 54, no. 5 (2025): 519–29. https://doi.org/10.1080/15374416.2023.2286595.

Hayes, Darren, Francesco Cappa, and Nhien An Le-Khac. "An Effective Approach to Mobile Device Management: Security and Privacy Issues Associated with Mobile Applications." *Digital Business* 1, no. 1 (2020): 100001. https://doi.org/10.1016/j.digbus.2020.100001.

Internet Matters, and BMG Research. *The Online Safety Act: Are Children Safer Online?* Internet Matters, 2026. https://www.internetmatters.org/hub/research/online-safety-act-report-2026/.

Japan Fair Trade Commission. *Mobile Software Competition Act Guidelines*. 2025. https://www.jftc.go.jp/file/MSCA_Guidelines_tentative_translation.pdf.

Lee, Mike. "Lee Introduces Bill to Protect Children Online, Hold App Stores Accountable." Mike Lee US Senator for Utah, May 1, 2025. https://www.lee.senate.gov/2025/5/lee-introduces-bill-to-protect-children-online-hold-app-stores-accountable.

Linarducci, P. J. "Bringing Secure Digital Identity and Payment Tools to More People." *Google*, June 4, 2026. https://blog.google/products-and-platforms/platforms/google-pay/secure-identity-payment-tools/.

Liu, Shuang, and Sarah Scheffler. "Adequately Tailoring Age Verification Regulations." Paper presented at CSLAW '26: Proceedings of the Symposium on Computer Science and Law. Version 2. March 3, 2026. https://dl.acm.org/doi/abs/10.1145/3788646.3789526.

Mariani, Adamo, Matteo Liberato, Anna Sperotto, and Antonia Affinito. "Analyzing Privacy Implications of Mobile Apps Data Collection across Age Groups." *20th International Conference on Network and Service Management (CNSM)*, October 28, 2024, 1–7. https://doi.org/10.23919/CNSM62983.2024.10814597.

Nagata, Jason M., Kristen E. Kim, Alicia W. Leong, Dimitri A. Christakis, Fiona C. Baker, and Lauren Hale. "Smartphone Use on School Nights in the Adolescent Brain Cognitive Development Study." *JAMA Pediatrics*, ahead of print, May 18, 2026. https://doi.org/10.1001/jamapediatrics.2026.1707.

Ofcom. *Children and Parents Media Use and Attitudes Report*. 2026. https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/2026-children-and-parents-report/children-and-parents-media-use-and-attitudes-report-2025-6.pdf?v=418231.

O'Leary, Lizzie, host. *Why He Sued Roblox*. What Next: TBD. Slate, March 15, 2026. https://slate.com/podcasts/what-next-tbd/2026/03/why-roblox-is-being-sued-by-nebraskas-attorney-general.

Online Safety Act 2023, c. 50 (2023). https://www.legislation.gov.uk/ukpga/2023/50.

Online Safety Amendment (Social Media Minimum Age) Act 2024. No. 127, 2024. Federal Register of Legislation, December 10, 2024. https://www.legislation.gov.au/C2024A00127/latest

Protecting Our Kids from Social Media Addiction Act. 2024 Cal. Stat. ch. 321 (S.B. 976). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB976.

Reader, Ruth. "How Mark Zuckerberg Is Flipping the Script on Kids' Safety Online." *POLITICO*, April 20, 2025. https://www.politico.com/news/2025/04/20/zuckerbergs-enlisting-the-gop-against-tech-rivals-apple-and-google-00295945.

Rescorla, Eric. *How Not to Mandate Device-Based Age Assurance*. March 27, 2026. https://educatedguesswork.org/posts/device-based-age-assurance/.

Rescorla, Eric, Zander Arnao, and Alissa Cooper. *Age Assurance Online: A Technical Assessment of Current Systems and Their Limitations*. Knight-Georgetown Institute, 2026. https://kgi.georgetown.edu/research-and-commentary/age-assurance-online/.

Sandle, Paul, Sam Tabahriti, and Sam Tabahriti. "Big Tech Firms Must Stop Young People Circulating Nude Images, Says UK PM Starmer." Media & Telecom. *Reuters*, June 8, 2026. https://www.reuters.com/business/media-telecom/big-tech-firms-must-stop-young-people-circulating-nude-images-says-uk-pm-starmer-2026-06-08/.

Schoenbaum, Hannah. *Utah Becomes the First State to Pass Legislation Requiring App Stores to Verify Age*. March 6, 2025. https://apnews.com/article/utah-app-store-age-verification-7e31de07ddca7b32cc82f7ead2c4adc9.

SensorTower. "State of Mobile 2025." 2026. https://sensortower.com/report/state-of-mobile-2025/download.

Similarweb. "Mobile vs. Desktop Traffic Market Share [June 2026]." July 9, 2026. https://www.similarweb.com/platforms/.

Stop Addictive Feeds Exploitation (SAFE) for Kids Act. S.7694A, 2023–2024 Reg. Sess. New York State Senate. https://www.nysenate.gov/legislation/bills/2023/S7694/amendment/A.

Thomas, Dexter, host. *Discord's New Age Verification Is about to Spy on Every Message*. Kill Switch. April 29, 2026.

https://podcasts.apple.com/us/podcast/discords-new-age-verification-is-about-to-spy-on-every/id1449757372?i=1000764254904.

Twenge, Jean. “I Tried to Protect My Kids from the Internet. Here’s What Happened.” *The Washington Post*, September 23, 2025. https://www.washingtonpost.com/opinions/interactive/2025/parental-controls-tech-companies-social-media-verify-age/.

United States. Congress. House. Committee on the Judiciary. Subcommittee on Antitrust, Commercial, and Administrative Law. *Investigation of Competition in Digital Markets: Majority Staff Report and Recommendations*. Washington, D.C., 2022. https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf.

Williams, Isaiah. “‘I Can’t Believe This Is Happening’: iPhone Users Are Threatening to Defect to Android over New iOS Age Verification Push — and I’d Do the Same.” *TechRadar*, March 26, 2026. https://www.techradar.com/phones/ios/i-cant-believe-this-is-happening-iphone-users-are-threatening-to-defect-to-android-over-new-ios-age-verification-push-and-id-do-the-same.

Winecoff, Amy, and Alissa Cooper. Knight-Georgetown Institute, 2026. *Age Assurance Rules: An Implementation Guide.* https://kgi.georgetown.edu/research-and-commentary/assigning-responsibility-for-age-assurance