



April 2024

Age Verification: The Complicated Effort to Protect Youth Online

Sarah Forland, Nat Meysenburg, & Erika Solis

Open Technology Institute

Last edited on April 22, 2024 at 12:51 p.m. EDT

Acknowledgments

This report would not have been possible without the help of several people who offered their valued time, advice, and expert knowledge to us: Prem Trivedi, Lilian Coral, David Morar, and Sydney Saubestre. We would also like to thank all of those who contributed to this work through interviews and the review process.

Editorial disclosure: The views expressed in this report are solely those of the authors and do not reflect the views of New America, its staff, fellows, funders, or its board of directors.

About the Authors

Sarah Forland is a senior research associate at New America's Open Technology Institute.

Nat Meysenburg is a technologist at New America's Open Technology Institute.

Erika Solis is a Google Public Policy Fellow at New America's Open Technology Institute.

About New America

We are dedicated to renewing the promise of America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Open Technology Institute

OTI works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.

Contents

Executive Summary	6
Introduction	9
Age Assurance and Age Verification	10
Age Verification Methods	11
Pursuing Kids Safety through Online Age Verification Legislation	13
State Legislation	13
Federal Legislation	16
International Efforts	17
Challenges with Age Verification	19
Technical Immaturity	19
First Amendment Implications—Restricting Access and Excluding Eligible Users	20
Data Privacy and Security Risks	21
Determining Scope of Responsibility and Level of Implementation	22
Cost of Compliance and Impact on Competition	23
Ease of Circumvention	23

Contents Cont'd

Social Media Platforms and Age-Appropriate Practices	24
Detecting and Verifying Under-Age Accounts	25
Age-Specific Design Features	25
Parental Controls	26
The Path Forward: Minimizing Potential Ramifications of Online Age Verification	27
1. Explore Alternative Solutions That May More Effectively Address Concerns Surrounding Youth Online Safety	27
2. Design for User Privacy and Choice When Building Age Verification Technology	28
3. Require Greater Transparency and Agency over User Experience	29
4. Understand That Content-Based Restrictions Will Have Unintended Consequences for People from Vulnerable Communities	30
5. Invest in Cross-Sector Research and Collaboration to Create Standardized Best Practices and Protocols for Age Verification	30
Appendix	32

Executive Summary

Legislators across the United States are contemplating age verification mandates as a way to limit the potential harms of online experiences for youth and restrict access to age-inappropriate material. While more efforts are needed to ensure children can safely and securely access online spaces, age verification mandates may actually pose more risks than benefits—resulting in unintended consequences for the constitutional rights, privacy, and security of *all* users.

Most age verification legislation is currently aimed at online content that faces age barriers in the real world. However, some legislators have gone further to target social media platforms. Given the outsized impact of widespread age verification requirements and the potential for serious unintended consequences, this report aims to demystify and clarify these key concepts related to online age verification.

Age Assurance and Verification Terminology

The terms *age assurance* and *age verification* are often used interchangeably but have different privacy and security implications—this can cause confusion, particularly when implementing legal mandates. Age assurance is generally used as an umbrella term to describe the different methods to vet the ages of users, and age verification implies authenticating a user’s age with a higher level of certainty, often through the use of government-issued identification. Currently, online operators implementing age restrictions must rely on either age assurance techniques or age verification via a government-issued ID. In practice, this poses the same challenges and risks as identity verification, which requires users to disclose their identity beyond their age.

Legislative Impact

Age verification laws impact all users, not just youth. As states begin to target social media with age verification requirements, the patchwork of legislation could complicate online services’ ability to comply. Age verification requirements can exclude users reluctant to disclose their government-issued ID or those without such ID, creating a chilling effect and raising additional barriers to access protected speech. If an online operator believes it cannot verify the ages of users with certainty, it may be inclined to censor or restrict what content is available for *all* users—or even suspend services within a state entirely—to avoid legal action and liability.¹ These challenges will only be amplified by age verification requirements for social media platforms, which for many people are a cornerstone of full social, economic, and political participation.

Implementation Challenges

Age verification requirements pose immense challenges to users and online operators. Currently, strict age verification—confirming a user’s age without requiring additional personally identifiable information—is not technically feasible in a manner that respects users’ rights, privacy, and security. For online operators, the mandated point of verification will significantly impact the cost, scope, efficacy, and risks of age verification legislation. In addition, age verification legislation and technologies are not ultimately foolproof, and neither option will completely stop under age users from intentionally or unintentionally accessing age-inappropriate content.

All children—and adults—should be able to safely and securely access online spaces that operate in a rights-respecting manner. Advancing kids’ safety online is complex and requires nuance. As state and federal legislators explore age verification as a method of improving youth experiences online, the Open Technology Institute offers key considerations for if legislators move forward with age verification and for navigating the potential ramifications of such mandates.

1. **Consider alternative solutions to age verification that may more effectively address concerns surrounding youth online safety.**

Improving youth experiences online requires a holistic approach. Alternative approaches to improving youth—and general user—online safety may more effectively and directly address concerns about access to age-inappropriate materials and the negative impact of online spaces. Age verification is no substitute for privacy protections and increased user transparency and control.

2. **Design for user privacy and choice when building age verification technology.** In online spaces in which age verification is absolutely necessary, strict age verification that optimizes user privacy through data minimization and user choice via standardizing third-party facilitation and best practices can be used to implement age restrictions.

3. **Require greater transparency and agency over user experience.** Platforms are moving ahead with alternative approaches to protecting youth from potentially harmful content and interactions online, such as limited asks for hard-identifiers, age-specific features, and parental controls. These approaches should be evaluated for both potential benefits (greater transparency and agency over online experiences) and risks (data privacy and constitutional concerns) to highlight promising techniques.

4. **Understand that content-based restrictions will have unintended consequences for people from vulnerable communities.** Content-based restrictions will face strict constitutional scrutiny and should be used sparingly to avoid allowing the politicization of content to drive mandates that change the nature of the internet and disproportionately impact vulnerable communities.

5. **Invest in cross-sector research and collaboration to create standardized best practices and protocols for age verification.** More research is needed to fully understand the potential impacts of age verification and implementation. Insights from industry, civil society, regulators, and users of all ages should be taken into consideration to create standardized best practices and protocols for age verification.

Introduction

In response to growing concerns about children’s safety online, legislators across the United States are contemplating age verification mandates as a way to limit the potential harms of online experiences and restrict access to age-inappropriate material. In 2023, more than 60 bills were introduced at the state and federal level requiring greater parental consent, age restrictions, or safety-by-design measures.² Half as many bills have already been introduced in the first few months of 2024.³ Most of these laws, passed and pending, target youth access to online adult content and sales that are age-gated “in real life.” Yet some states are going further to apply age verification requirements to social media, responding to concerns from parents and teens, schools, legislators, and regulators about children’s experiences online.⁴

While more efforts are needed to ensure children can safely and securely access online spaces, current technical limitations often mean that age verification mandates may actually pose more risks than benefits. Many social media platforms and other online operators already implement a wide range of age assurance practices to comply with existing laws and uphold their own terms and conditions. These methods aren’t perfect, but mandating age verification, which often necessitates sharing government-issued identification, can negatively impact users’ constitutional rights, privacy, and security.

Previous attempts to protect minors from harmful material online through content restrictions and required age verification—such as the **1996 Communications Decency Act** and **1998 Child Online Protection Act**—have largely been ruled unconstitutional by federal courts for being overly broad, restricting freedom of expression, and limiting access to protected speech.⁵ These new laws are likely to face the same fate, especially as some of the champions of these bills raise concerns about veiled attempts to restrict access to critical, and often politicized, information about gender, sexuality, and reproductive health care.⁶

Given the outsized impact of age verification requirements and the potential for serious unintended repercussions, it is important for users, lawmakers, regulators, industry, and civil society to understand the recent push toward age verification and its implications for how children and adults use and access content online. This report aims to demystify and clarify key concepts related to online age verification by providing a digestible survey of (1) current terminology and practices; (2) recent state and federal efforts requiring online age verification; (3) legal, technical, and social implementation challenges; (4) social media age-based features; and (5) recommendations for minimizing potential harms of age verification moving forward.

Age Assurance and Age Verification

While there are “no universally recognized legal definitions” for these terms, *age assurance* is generally used as an umbrella term to describe online operators’ methods to vet the ages of users and implement age restriction laws online.⁷ Any—or a combination of the following—age assurance techniques can be used to determine a user’s age range or a binary statement about their age (such as this person is or is not 21+ years old):

- **Age-gating/age-screening**, or asking a user to self attest their age through checking a box or inputting a date of birth to confirm they are or older than the necessary age to access content;
- **Age estimation**, or estimating a user’s age by analyzing their online profile, activity, history, or facial data;
- **Third-party verification**, or trusting a third-party to verify a user’s age, using methods such as referencing linked accounts, vouching of age from parents or other users, or inspecting hard identifiers such as government-issued identification; and
- **Age verification**, or directly inspecting identifiers such as government-issued identification or biometric data to confirm a user’s age.

The terms *age assurance* and *age verification* are often used interchangeably—though this can cause confusion, particularly when implementing legal mandates. **Age assurance** includes a variety of methods to “establish, determine, or confirm a user’s age with some level of confidence,” according to the Digital Trust & Safety Partnership.⁸ These methods offer varying degrees of accuracy, authenticity, reliability, and verifiability. **Age verification** is a subset of age assurance, which implies authenticating and confirming a user’s age with a higher level of certainty, often through the use of government-issued identification. As such, age verification in practice often means identity verification, requiring a user to disclose their identity beyond their age.

It is important to note that identity verification has implications for user privacy that differ from the implications of age verification. **Identity verification** requires a user to provide personally identifiable information about themselves to establish and verify their identity. Or as the National Institute for Standards and Technology (NIST) defines it, “the process of confirming or denying that a claimed identity is correct by comparing the credentials...of a person requesting access with those credentials previously proven...and associated with the identity being claimed.”⁹

On the other hand, age verification can simply mean establishing or verifying a person's age. The Age Verification Providers Association (AVPA) defines age verification as "the process of checking the age of an internet user, without necessarily needing to know their identity."¹⁰ This distinction around identity is critical. Requiring a user to disclose their identity is in itself a privacy intrusion, and online handling and processing of data can put personal information at risk. Additionally, forced identity disclosure can create a chilling effect on speech and exclude people who lack appropriate identification from online spaces and services.¹¹ Online operators implementing age restrictions currently must rely on either age assurance techniques or age verification through the use of a government-issued ID—which in practice poses the same challenges and risks as identity verification. To help maintain these distinctions, this report will use *strict age verification* to refer to age verification methods that do not require verifying a person's identity. However, the reality is that **limitations** in today's technology do not enable this type of strict age verification.

Age Verification Methods

Young online users are subject to the Children's Online Privacy and Protection Act (COPPA), which requires online operators to obtain parental consent for their collection, use, or disclosure of personal data for children under 13 years old.¹² To, presumably, avoid being subjected to COPPA requirements, social media platforms—as well as many other websites—often require account holders to be older than 13 years of age.

As such, current age assurance practices mimic the approved methods of parental consent outlined by the Federal Trade Commission's COPPA standard for acceptable methods of obtaining parental consent.¹³ These methods include signing and submitting a consent form; using a credit card, debit card, or online payment system; calling a toll free number; connecting via video conference; providing a copy of government-issued ID that can be checked against a database; answering multiple knowledge-based questions; and verifying a photo ID with a real-time photo using facial recognition technology.

Each age assurance method and implementation strategy comes with its own trade-offs for user rights, data privacy, and security. Below is a non-exhaustive survey of age assurance methods, categorized by the underlying age assurance techniques outlined above. These methods are listed generally in order of lowest to highest level of assurance, broadly reflecting AVPA's levels of age assurance and levels of assurance outlined in NIST's Digital Identity Guidelines.¹⁴ However, levels of assurance will vary based on accompanying implementation practices.

Age Assurance Methods

Method	Category	Description	Example*
Self-Declaration	Age Gate/Screen	A user self attests their age by checking or inputting their date of birth.	Instagram asks users to submit their date of birth upon sign-up to confirm they are 13+.
Account-Based Assurance	Third-Party Verification	User's account on an age verified service is used to vouch for their account on a different service.	X partners with Au10tix to verify paid users.
Vouching	Third-Party Verification	Parent or other users vouch that the user in question is of a certain age.	Meta offers social vouching in which users can select three people to confirm their age. TikTok allows users to submit a photo with their parent, guardian, or trusted adult over the age of 25 as part of an age appeal.
Cookie Tracking	Third-Party Verification	Browser cookies are used to determine whether or not the user has already completed a qualifying age verification check.	AgeVerify previously offered a service that used browser cookies to track individuals that had successfully completed an age-gate process to avoid users completing multiple age verification checks.
Browser Storage	Third-Party Verification	Browsing session storage is used to identify if a user has already completed a qualifying age verification check or not.	AgeVerify, which previously used cookie tracking to implement age verification across multiple sites, now uses browser storage to identify users that have already completed an age verification process.
AI Facial Age Estimation	Age Estimation	AI analyzes a still or live photo of the user's face to estimate their age.	Yoti, which currently partners with Meta, offers AI facial age estimation.
Social Graph Age Estimation	Age Estimation	This method is also called social proofing or algorithmic profiling, where AI analyzes a user's social graph (online connections to other users) and online activity to estimate their age.	TikTok scans users' public videos to help ensure ages are accurately reported.
Liveness Detection	Age Estimation	Users may submit a photo or video while holding written specific information or saying a specific word or phrase. AI can also be used to analyze the age of the user shown in the video or phone. (This technique is usually used in coordination with another age verification method to prove the user is the person completing the age verification check.)	Yubo asks users to take a real-time photo in the app that is then analyzed using Yoti technology to estimate the age of the user.
Credit Card	Third-Party Verification	Users submit their credit card information to confirm their age.	To access age-restricted content or update an account to meet age requirements, Google allows users to submit a photo and either a credit card or government-issued ID to confirm their age.
Government- Issued Identity	ID Verification	Users submit a government-issued ID, such as a driver's license or passport, to verify their identity.	X offers voluntary ID verification for premium users through government-issued IDs.
Government ID and Current Photo	ID Verification	Users submit a government-issued ID, such as a driver's license, passport, or residency card, along with a current still or live photo to verify their identity.	Roblox is testing a new age ID verification feature that asks users to submit a current photo and a valid government-issued ID.
Mobile Phone Registration /SIM Card	Third-Party Verification	To unlock default age restrictions or parental controls on new phones and SIM cards, users must verify their age.	O2, the United Kingdom's largest mobile network provider, filters and blocks 18+ websites, requiring users to verify their age before accessing. In Japan, LINE requires users to verify their age through their SIM card or mobile phone registration.
Token-Based	Third-Party Verification	Users verify their identity and age with a third party in exchange for a token that can be stored in a digital wallet. The token can be used to verify age on platforms and websites without requiring users to re-enter credentials or submit identification.	Yoti offers reusable age verification checks, or age tokens, that allow users to verify their age across browsers and devices.
Zero-Knowledge Proof (Double-Blind Systems)	Third-Party Verification	A zero-knowledge proof or double-blind system uses a third-party facilitator to connect a user's age verification provider and website in a data minimizing capacity. The third-party facilitator confirms with the website that a user meets the age or age range requirements, but shares no other information about the user and collects no information about the site requesting the verification.	Researchers from France's CNIL built "a possible implementation of an age verification system that allows accessing restricted websites without sharing other personally identifiable data."

*Note: Companies often implement a variety of age verification methods; listings in the example column do not represent a comprehensive view of all methods employed by the highlighted platform or company.

NEW AMERICA

Pursuing Kids Safety through Online Age Verification Legislation

State and federal legislators across the United States—and around the world—are attempting to address the current loopholes in age assurance techniques by requiring online operators to verify the ages of their users (often through government-issued identification).

State Legislation

In 2022, Louisiana became the first state to mandate age verification via government-issued ID for users accessing adult content online.¹⁵ In 2023, Arkansas, Mississippi, Montana, North Carolina, Texas, and Virginia followed suit.¹⁶ Currently, these bills require online operators that “distribute material harmful to minors” and “contain a substantial portion” (or greater than 33.3 percent) of such material to verify users’ ages. This type of requirement can impact a variety of online operators, but is mainly intended to reduce youth access to online adult content and sales that are age-gated in real life. However, Utah and Connecticut, and additional laws in Louisiana and Arkansas,¹⁷ went further with age verification mandates, extending the requirements to social media platforms and their users.¹⁸ This trend raises two immediate concerns.

First, age verification laws impact all users, not just youth. Age verification requirements can exclude users reluctant to disclose their government-issued ID or those without such ID, creating a chilling effect on their speech and additional barriers to accessing protected speech. If an online operator cannot, with certainty, verify the ages of users, it may choose to censor or restrict content that is available for *all* users—or even suspend services within a state entirely—to avoid legal action and liability.¹⁹ While lawmakers may intend to only apply restrictions to specific content or to overall platform access to users of a certain age, the impact of broad and vague age verification legislation can be far reaching. For example, in response to age verification requirements, Pornhub, one of the largest adult content operators, removed access to all users in Mississippi, Utah, and Virginia.²⁰

Second, since many of these laws are enforced through an individual’s right to private action, the courts’ full interpretation of the law and how it applies to particular content and online spaces is unclear and will unfold only as lawsuits against companies are brought forward. As courts determine the scope of “material harmful to minors,” groups and topics that are already vulnerable to politicization may be targeted—as seen in the recent efforts to ban LGBTQ+

content from libraries, remove critical race theory from school curriculum, and restrict access to reproductive health care sources.²¹

Creating barriers to speech and targeting access to specific content raises serious constitutional concerns. Even age-gating scenarios meant to reduce youth access to adult content have previously been found to be unconstitutional for overbreadth of impact.²² While there is a compelling government interest to restrict youth access to age-inappropriate content, the movement still faces strict constitutional challenges. These challenges will only be amplified by age verification requirements for social media platforms, which have become, for many people, a cornerstone of full social, economic, and political participation in modern life.²³ Legal challenges have already been brought forth in some states, but legislators at the state and federal level are nevertheless continuing to pursue age verification mandates.

→ POTENTIAL LEGAL CHALLENGES

States are leading the way on age verification requirements, creating a patchwork of legislation that will change how every user across the United States accesses content online.²⁴ While much of the passed and pending pieces of state legislation share numerous characteristics, three categories of core differences between them demonstrate the potential legal challenges that lie ahead and will complicate how online operators respond to and comply with new mandates: (1) loosely defined terminology and proposed age verification methods; (2) various targeted online operators; and (3) unclear enforcement outcomes.

Loosely Defined Terminology and Proposed Age Verification Methods

Variations in terms and definitions across legislation will affect age verification processes, as each method poses unique data privacy and security risks and faces potential constitutional hurdles. Age verification does not have a universally accepted legal definition in the United States, and is often used interchangeably with age assurance. As a result, the

understanding of what age verification actually entails varies. Of the bills passed in 2023, the majority require “reasonable age verification” or confirming that a user is 18+ or not a minor as defined by that state. Yet, it is unclear exactly what constitutes “reasonable” age verification practices, or what complying with the widely adopted standard of “commercially reasonable” methods for age verification actually requires.²⁵ Several passed bills identify digitized identification cards or any government-issued identification as an acceptable form of age verification. Some laws (specifically those in Louisiana, Mississippi, and Montana) allow for the use of private transactional data—such as from mortgage, employment, or educational records—to confirm a user is 18 years or older.²⁶ In other cases, such as North Carolina, Texas, and Utah, laws do not define age verification, leaving the term open to interpretation.²⁷ Virginia’s law goes further, requiring both “age and identity verification” to access material that may be harmful to minors.²⁸

Various Targeted Online Operators

Determining which online operators must comply with age verification mandates will determine the cost, efficacy, potential risks, and level of invasiveness of these mandates.

Passed and introduced age verification bills differ in the types of online operators they target. Following Louisiana’s lead, Mississippi, Montana, North Carolina, and Arkansas target online operators containing a “substantial portion” of “material harmful to minors.”²⁹ Other bills, such as Utah Senate Bill 152, Connecticut Senate Bill 3, Louisiana Senate Bill 162, and Arkansas Senate Bill 396,³⁰ target social media companies, each offering their own definitions.³¹ Uniquely, Texas’s bill imposes age verification on digital service providers, defined as “a website, application, program, or software that collects or processes personal identifying information with Internet connectivity.”³²

Unclear Enforcement Outcomes

States take a varied approach to enforcing age verification mandates, which can lead to a range of cascading effects as online operators assess risks of operating in an area and courts handle litigation. The majority of bills passed and introduced create a right of action for private citizens to sue companies and impose civil and administrative penalties for online operators that fail to comply with age verification requirements and allow minors to access harmful material. Since these laws are based on private rights of action, the full extent of their impact will be uncertain until litigation occurs. Some states enable Attorney General action, such as those in Connecticut and Arkansas.³³ However, some states go further in enforcement, introducing age verification bills with associated criminal charges, ranging from a misdemeanor (Indiana and Wyoming) to a Class C Felony (Tennessee and Ohio).³⁴

As states move forward with differing age verification bills, online operators will face challenges navigating the patchwork of laws that come into effect. As with previous attempts to require age verification, federal courts have blocked laws in Arkansas and Texas for being unconstitutional.³⁵ Courts also blocked the California Age Appropriate Design Code in part for its inadvertent age verification requirements, since the law mandated additional safeguards for all web services “likely” to be accessed by users under 18 years old.³⁶ However, legal challenges in Utah and Louisiana were dismissed on the grounds that the filers sued state officials, who do not have enforcement authority, as those laws enable a private right of action for users.³⁷ Most recently, a federal appeals court upheld Texas’s age verification law, overturning a lower court ruling.³⁸ Altogether, competing court decisions and precedents show that the legality of age verification requirements for either online adult content or social media is an unsettled question.

Federal Legislation

National governments are also taking on the challenge of improving online safety for youth through a variety of methods, including age verification. Age verification requirements implemented at a national level will have a rippling impact across global online spaces. As online operators reconfigure their internal

processes for compliance, national legislation could set new precedents for how users—even those beyond their borders—access content online.

At the federal level in the United States, age verification and youth online safety bills have focused on social media companies. In previous sessions, a range of bills, including the Making Age-Verification Technology Uniform, Robust, and Effective (MATURE) Act and Protecting Kids on Social Media Act sought to implement age restrictions and age verification, respectively, on social media platforms.³⁹ Neither of these bills have been reintroduced in 2024.

The most prominent piece of federal legislation is the Kids Online Safety Act, which would establish a “duty of care” for platforms, or establish a legal responsibility for knowing or reasonably knowing if the user is a minor and taking the appropriate steps to mitigate and reduce online risks.⁴⁰ Initially introduced in May 2023, the bill faced criticism for its restrictions on free speech and inadvertent age verification requirements.

The bill has since been amended twice, garnering bipartisan support for tackling kids safety online.⁴¹ However, criticisms of the bill remain.⁴² The most recent iteration of the bill removes explicit age verification requirements and includes a provision that would require a study “evaluating the most technologically feasible methods and options for developing systems to verify age at the device or operating system level.”⁴³

International Efforts

Countries outside the United States are looking to age verification technologies to enforce online restrictions on content and services that may be harmful to children. And they are seeing similar challenges and criticism that face U.S. efforts.

The United Kingdom’s Online Safety Act of 2023 requires and places responsibilities on social media platforms to take the necessary measures to verify a user’s age.⁴⁴ This legislation is facing backlash for potentially compromising user privacy and safety online.⁴⁵

Australia’s eSafety Commissioner submitted an age verification roadmap weighing potential methods and impact.⁴⁶ Based on the findings, the Australian government decided against implementing any age verification measures citing privacy and security concerns, and instead suggested alternative avenues to creating safer online environments for children.⁴⁷

Similarly, in 2022, the French Commission on Information Technology and Liberties (Commission Nationale de l’Informatique et des Libertés) released a report concluding, “there is currently no solution that satisfactorily” can provide

reliable age verification and complete coverage of the population while respecting user data privacy and security.⁴⁸

The European Union's euCONSENT project is attempting to develop an open, secure, and interoperable solution network for age verification and parental consent.⁴⁹ The project is currently in the second phase of its pilot, and it could provide valuable insight into applying age verification requirements.

Challenges with Age Verification

As governments around the world explore better ways to ensure children can safely and securely access online spaces, age verification requirements continue to pose a number of challenges to users and online operators. Such challenges include: technical immaturity; first amendment implications—restricting access and excluding eligible users; data privacy and security risks; determining scope of responsibility and level of implementation; cost of compliance and impact on competition; and ease of circumvention.

Technical Immaturity

As of this report’s publication, **strict age verification—confirming a user’s age without requiring additional personal identifiable information (PII)—is not technically feasible in a manner that respects users’ rights, privacy, and security.** In 2022, the French Commission on Information Technology and Liberties (CNIL) investigated six common solutions for online age assurance, including payment card validation, facial analysis, offline verification, identity documentation, government-provided tools, and inferential verification.⁵⁰ CNIL’s report examined whether these solutions provided “sufficiently reliable verification, complete coverage of the population, and respect for the protection of individuals’ data and privacy and their security” and found that “there is currently no solution that satisfactorily meets these three requirements.”

Australia’s eSafety Commission released an in-depth roadmap for age verification, which also found that “each type of age verification or age assurance technology comes with its own privacy, security, effectiveness, and implementation issues.”⁵¹ The Australian government noted that age assurance technologies are too immature to work effectively while balancing user privacy and security, ultimately suggesting alternative methods of improving children’s safety online, such as industry codes, increased platform transparency, and greater parental support.⁵²

→ FACIAL AGE ESTIMATION

Facial age estimation, or using artificial intelligence (AI) to analyze the geometry of a user's face in a still or live photo to estimate their age, is gaining popularity as an age-gating and verification method. In 2022, Meta began testing new age verification methods on their services, including facial age estimation, and found that 81 percent of people chose this method when presented with a menu of options.⁵³ The euCONSENT project also found facial age estimation to be the most popular age verification method offered—chosen by 68 percent of all participants.⁵⁴ In 2023, **Yoti**, the **Entertainment Software Rating Board**, and **SuperAwesome** submitted an application to approve facial age estimation as an Federal Trade Commission (FTC)-approved method for obtaining parental consent under its Children's Online Privacy Protection Rule.⁵⁵ Proponents of this method stated it offers an easy and less-intrusive way to verify a user's age without asking for formal identification.⁵⁶ Meanwhile, opponents of the method raised concerns regarding privacy and accuracy for determining specific ages rather than age ranges—as well as determining the ages of people of color and transgender, nonbinary, and disabled people, who may be disproportionately subject to false negatives or positives.⁵⁷ In March 2024, the FTC denied the application without prejudice in a 4–0 vote.⁵⁸ In September 2023, the same technology was submitted to the National Institute of Technology for evaluation, which is forthcoming.⁵⁹

It should be emphasized there are no available technologies that verify age in a private and secure manner, much less any that could do so at the scale required by large social media platforms.

First Amendment Implications—Restricting Access and Excluding Eligible Users

Current practices of age verification often require disclosing government-issued ID, and users who are hesitant to disclose or those without such ID face restricted access to content, anonymity, and privacy.

Given current technological limitations, age verification mandates require online operators to verify the age of every user (often through the use of government-issued identification). If an online operator believes they are unable to undertake this task with certainty, it may feel obligated to censor or restrict content available for all users to avoid legal action and liability.⁶⁰ As a result, many age verification laws aimed at protecting children inadvertently limit access to content and infringe on all users' First Amendment rights.

Previous Congressional attempts to protect minors from harmful material online through content restrictions and required age verification failed to pass constitutional muster. Supreme Court rulings found the Communications Decency Act and Child Online Protection Act unconstitutional for being overly broad, restricting freedom of expression, and limiting access to protected speech.⁶¹ Through these cases, the Court also acknowledged that age verification mandates would impose significant costs on commercial entities and limit access of adults without acceptable identification. Current limitations on commercially effective and available tools may also impact the Court's willingness to accept any new online age verification requirements aimed at protecting children's safety online.⁶² It is also important to note, that while the Supreme Court has established the government's ability to regulate material deemed harmful to minors, particularly obscene material, children are not completely exempt from First Amendment rights to protected speech.⁶³

In addition, those that lack any acceptable form of identity to prove their age may be excluded from accessing content protected by the First Amendment under traditional methods of age verification simply because they do not have access to a government-issued ID or credit card. Youth between the ages of 14 to 16 years old often do not hold any official form of government identification, and those under the age of 18 are unable to hold credit cards. Millions of adults who are 18 years of age and older do not hold a valid government-issued photo identification.⁶⁴ Additionally, the Federal Deposit Insurance Corporation's 2021 *National Survey of Unbanked and Underbanked Households* found that 28.5 percent of households did not have a credit card and 4.5 percent were unbanked.⁶⁵ Age verification requirements also leave no space for users who do not wish to identify themselves online, threatening individuals' right to anonymous speech, which has long been upheld by the Supreme Court.⁶⁶

Data Privacy and Security Risks

Most age verification methods are at odds with data minimization, posing significant risks to user data privacy and security. Recent age verification laws require that online operators cannot knowingly retain users' personal information, but the act of verifying user ages itself can put personal and sensitive data at risk. For instance, operators verifying users' ages through

government-issued ID or credit card information put data at risk if secure processes are not in place for use, collection, processing, storage, or deletion of PII. This, in turn, increases the risk that such sensitive data could be merged, stolen, sold, or turned over as part of legal proceedings.⁶⁷

At the same time, operators who choose to verify ages through estimation or inference models may increase surveillance and monitoring of users' online activity, such as their content, engagement, social networks, geographic location, screen time, linked accounts, and browsing history. Subjecting users to such intrusive practices may result in a chilling effect that suppresses online speech and enables the potential collection, use, or sale of user activity data.

Determining Scope of Responsibility and Level of Implementation

The point of verification—whether that be via an online operator or platform, app-store, device, operating system, or internet service provider (ISP)—will significantly impact the cost, scope, efficacy, and risks of age verification mandates. Currently, most age verification legislation targets online operators and platforms—with the exceptions of Idaho and Tennessee, which target devices.⁶⁸ While NetChoice, a coalition of trade associations, eCommerce businesses, and online consumers, has challenged attempts to implement age verification requirements, Meta and Pornhub have recently come out in support of different approaches to online age verification. Meta's Global Head of Safety argued that app stores should play a larger role in age verification, while Pornhub representatives supported device-level age verification.⁶⁹

Selecting the technological intervention point at which age verification is required has implications for the degree of invasiveness of the policy. For example, implementation via online platforms could create an onerous verification system for users that puts their data at greater risk. Implementation at the app-store level leaves large gaps in coverage because it would not encompass non-application points of access like websites. At the device level, age verification could have implications for users' non-online activities and fail to account for multiple users. Similarly, requiring ISPs to verify age does not account for multiple users and necessitates invasive data monitoring and collection practices. More research is needed to fully explore the consequences of mandating age verification at any level of application.

Cost of Compliance and Impact on Competition

Age verification mandates would impose costly barriers to entry for start-ups and smaller operators. Such costs could unintentionally bias the market toward larger, more established companies that are better positioned to implement age verification and undertake the associated costs. Companies unable to effectively meet requirements may be forced to pull their services from jurisdictions with age verification legislation.

Most age verification laws, both passed and pending, require companies to institute any “commercially reasonable” age verification techniques—yet strict age verification or age verification through the use of government-issued identification can be costly. In a *POLITICO* article, Mike Stabile, the director of public affairs for the Free Speech Coalition, states that age verification costs operators “around 65 cents per verification,” which can be exorbitant for many companies processing hundreds of thousands of users, potentially each time they begin a new session.⁷⁰ A February 2024 report by Engine, a start-up trade association, details how the direct and indirect costs of age verification requirements will make it more difficult for start-ups and smaller companies to compete.⁷¹ The report identifies costs such as age assurance product creation and integration, additional staff, data testing and training, cybersecurity, and the potential cost of data breaches.

Ease of Circumvention

Age verification legislation and technologies are not foolproof—nor will they completely stop underage users from intentionally or unintentionally accessing age-inappropriate content. Despite the efforts of legislators and online operators, users can still use tools like virtual private networks (VPNs) to bypass age verification.⁷² In China, where age verification is required to enforce online gaming limits, users evade restrictions through a variety of methods.⁷³ Tech giant Tencent found that users can evade age verification by borrowing the device of a parent or adult or by buying, renting, or trading verified adult accounts.⁷⁴ South Korea, which has similar limits for online gaming, also found children were using their parents’ identification to bypass age restrictions.⁷⁵

Further, as the technology develops, it’s uncertain how users will be able to use generative AI to circumvent age verification methods. For example, users could use realistic filters that can alter the age a person is perceived as in images and videos, or they could generate an image of an accepted identification document. Relatedly, the Supreme Court has also considered users’ ability to evade age verification tools as part of the rationale for finding mandates unconstitutional.⁷⁶

Social Media Platforms and Age-Appropriate Practices

In response to concerns about children's experiences online from parents and teens, schools, legislators, and regulators, state and federal age verification legislation is beginning to focus on social media platforms.⁷⁷ Growing evidence shows that while not inherently bad for youth, social media can facilitate and exacerbate challenges to children's mental health and safety online.⁷⁸ While more efforts are needed to ensure children can safely and securely access online spaces, age verification mandates present various challenges and may not actually address the root concerns surrounding social media use.

Already, websites and social media platforms implement a variety of age assurance practices to enforce previously established legal age restrictions—such as the Children's Online Privacy Protection Rule (COPPA) or age restrictions related to online gambling and alcohol and tobacco sales—and to uphold their own account age requirements. For example, when age restrictions are mandated by law, online operators may use hard identifiers such as photo ID or credit cards to confirm a user's age, which is similar to age assurance practices taking place in the physical world.

In the absence of age limits set by law, such as platform's account holder age requirements, many platforms and websites rely on self-declaration. This is usually done by asking users to input their date of birth when creating an account, link to an existing account with date of birth information, or simply check a box to confirm that they are the required age.

However, these methods aren't foolproof, as users can simply declare they are of the required age when they are not. Age verification legislation intends to close these loopholes but leaves online platforms grappling to respond to concerns about children's access to social media and age-inappropriate material while minimizing potential risks of age verification.

As a result, platforms have employed a variety of strategies to create safer online spaces for children and teens, such as requiring age verification only when an account holder is suspected to be underage, introducing age-specific features for users, and creating parental controls. These strategies have their own trade-offs and considerations for user rights, data privacy, and security, but they may offer insight for more direct and effective strategies for promoting kids safety online than those of age verification mandates.⁷⁹

Detecting and Verifying Under-Age Accounts

To identify users who do not self-declare their age accurately, some social media companies are incorporating measures to flag when a user may be under the required age. For example, TikTok scans public videos of users to help determine account holders' ages.⁸⁰ Meta uses artificial intelligence to detect underage account holders based on account activity and linked profiles.⁸¹ Additionally, both Meta's Instagram and Facebook platforms allow users to report accounts suspected to be held by an underage user.⁸² If a user tries to change their self-reported age or has been identified as being underage, platforms, including **Pinterest**, **Discord**, **TikTok**, and **Google**, require users to verify their age with a government-issued ID, credit card, or a live photo.⁸³ When users try to edit their account age from under 18 to over 18 years old, Meta's Instagram requires them to verify their age by submitting a government-issued ID, recording a video selfie to be analyzed by age-estimation AI, or asking mutual friends to vouch for their age.⁸⁴ This strategy may reduce the personal or sensitive data that users need to share with a platform to verify their age by only requesting verification of account holders suspected of being under the required age. However, methods used to detect these underage account holders may subject users to intrusive surveillance and monitoring of online activity and incorrectly flag account holders as being underage.

Age-Specific Design Features

Some platforms employ age-specific features to protect youth from potentially harmful content and interactions online. For example, Roblox is working to incorporate an age verification feature that will allow users 13 years of age and older to submit a government-issued photo ID and a selfie to verify their age to "access innovative social capabilities and age-appropriate content."⁸⁵ Enabling account restrictions on Roblox will lock an account's contact settings to block messages and chats from other users and limit play to experiences recommended for all ages.⁸⁶

Google offers a suite of digital well-being tools that allows all users to set daily limits and timers on apps, customize or turn off notifications, and set bedtime reminders—some of which are turned on by default for users who are 13 to 17 years old on YouTube.⁸⁷ In addition, Google has specific ad policies for teens that restrict personalized ads or ads containing sensitive content.⁸⁸

Snapchat implements specific default settings for teens, including limiting contacts to friends and existing phone contacts, restricting location sharing, and sending in-app reminders about privacy and safety settings.⁸⁹ Similarly, TikTok has a variety of age-specific features, such as prohibiting users under 13 years old from posting videos or comments, setting accounts held by 13 to 15 year olds to

private by default, and restricting live streaming and direct messaging for users under the age of 16.⁹⁰ In March 2023, TikTok introduced new age-specific features, including an automatic 60-minute screen time limit for users under 18 and created a screen time dashboard and controls for all users.⁹¹

In January 2024, Meta released new policies for teens, hiding age-inappropriate content, limiting content recommendations, and defaulting content recommendations to the most restricted settings.⁹² While these features help customize a safer and healthier online experience for young people, these features are not activated unless an account is created with the correct age.

Parental Controls

Companies are also creating more opportunities for parents to play a greater role in supervising their child's online activity. Many platforms already implement options for parents to set restrictions, monitor, enable permissions, and link accounts for their children's accounts.

TikTok's Family Pairing allows parents to link their TikTok account to their child's account to manage settings for various features, including account discoverability, searches, direct messaging, and screen time.⁹³ Similarly, Google's Family Link allows parents to manage parental controls such as SafeSearch and edit settings on YouTube Kids and YouTube accounts.⁹⁴

Apple's Family Sharing allows parents to create Apple IDs for their children and set parental controls and receive warnings about sensitive content sent or received by a child's account.⁹⁵ In 2022, Snapchat introduced its Family Center tool that allows parents to view their teen's privacy and safety settings, manage parental controls, and restrict sensitive content.⁹⁶ Likewise, Discord's Family Center allows parents to see who their child is talking to on the platform, what forums of which they are a part, and newly added friends.⁹⁷ In 2023, Meta began launching new parental supervision features on Facebook and Instagram that allow parents to see with whom their child is friends or messaging through both apps.⁹⁸

While parental controls offer greater insight and supervision into their child's online life, these controls may negatively infringe upon a young person's privacy and enable unnecessary surveillance of their online activity.

The Path Forward: Minimizing Potential Ramifications of Online Age Verification

All children—and adults—should be able to access online spaces and interactions safely, securely, and in a rights-respecting manner. The conversation around advancing kids' safety online is complex and requires thoughtful nuance to ensure strategies address core concerns. Age verification requirements can create a cascading impact on how all users access online content, as each age assurance and verification method comes with its own trade-offs for user rights, data privacy, and security.

Alternative approaches that optimize user choice, privacy, and control over their online experience may be more feasible and efficient at improving children and teen safety online than age verification mandates. As state and federal legislators explore age verification, the Open Technology Institute offers five recommendations for navigating potential ramifications of such mandates and for moving forward on addressing youth safety online.

1. Explore Alternative Solutions That May More Effectively Address Concerns Surrounding Youth Online Safety

Improving youth experiences online requires a holistic approach. Using a mix of alternative methods to improve youth—and general user—safety online may more effectively and directly address concerns about access to age-inappropriate materials and the negative impact of online spaces. Ultimately, age verification is no substitute for privacy protections and increased user transparency and control.

Growing concerns over social media's impact on youth mental health and well-being have driven the bulk of age verification and other youth-focused online safety bills.⁹⁹ Yet, these concerns are complex and no single technology solution can or will adequately address what are ultimately social challenges.¹⁰⁰ It is important to evaluate whether or not age verification requirements can effectively address the core concerns before moving forward with legislation.

Given the challenges and risks of age verification mandates, more feasible and effective methods for advancing children's safety online should be explored. First and foremost, comprehensive federal data privacy legislation, such as the [**American Data Privacy Protection Act**](#), remains the best method for protecting children, and all users, online.¹⁰¹ Such legislation would require stronger data minimization, limit the ability of companies to use the data they do collect, and create special protections for sensitive data like biometric information and precise geolocation data.

Other avenues, such as requiring platform transparency, customizable design features, or **safety-** and **security-by-design** principles, can offer users greater insight and control over the algorithms that impact their experiences online while standardizing a base level of data privacy and security. These methods could allow parents, youth, and all other types of users to tailor their default settings and the content they see online to better fit their needs.

2. Design for User Privacy and Choice When Building Age Verification Technology

In online spaces in which age verification is absolutely necessary, strict age verification that optimizes user privacy through data minimization and user choice via standardizing third-party facilitation and best practices can be used to implement age restrictions.

Age verification is incompatible with user needs and expectations for anonymity online and is likely to raise constitutional concerns. Mandates for age verification can infringe on user rights and put their privacy at risk. This is especially concerning as current age verification practices require users to share a government-issued identification, which could disproportionately impact vulnerable communities and access to politicized content. In spaces that require strong authentication needs or present clear precedent for age-based restrictions (such as engaging in online gambling or purchasing alcohol and tobacco products), strict age verification that uses data minimization principles and third-party facilitators can offer a rights-respecting method for implementing age restrictions.

Although the French Commission on Information Technology and Liberties (CNIL) concluded that no solution fully met their privacy criteria, their 2022 report discusses a proof of concept that shows it is possible “through a third-party system, to guarantee the protection of the individual’s identity and the principle of data minimisation, while maintaining a high level of assurance on the accuracy of the data transmitted.”¹⁰² Using two cryptographic concepts (group signatures, and zero knowledge proofs), researchers built “a possible implementation of an age verification system that allows accessing restricted websites without sharing other personally identifiable data.”¹⁰³ In other words, a system could be used in which the website only learns the age (or age range) of the visitor and the age verifier learns nothing about the site requesting the verification. This work shows that privacy-respecting age verification is possible via the use of existing and well-understood cryptographic principles.

Standardization of strict age verification can foster a varied ecosystem of third-party age assurance providers that enables greater user choice in who is verifying their age, promotes greater safety and security measures through competition,

and avoids concentrating verification solely within a few large tech companies. However, little conclusive work has been done so far in this area.¹⁰⁴ Even if a standard is agreed upon, there must be enough critical mass behind its use to actually make such a system useful for every type of site that may need to verify a user's age. As CNIL demonstrated, it is already technically possible to build an age verification system that assures privacy, but in the absence of an established and widely adopted protocol, it is unlikely that strict age verification can be widely done at scale in privacy-preserving ways.

Until there is a secure standard, age verification should be accompanied by security- and privacy-by-design practices, and online operators should offer users a variety of methods to confirm their age.

3. Require Greater Transparency and Agency over User Experience

Platforms are moving ahead with alternative approaches to protecting youth from potentially harmful content and interactions online, such as limited asks for hard-identifiers, age-specific features, and parental controls. These approaches should be evaluated for both potential benefits (greater transparency and agency over online experiences) and risks (data privacy and constitutional concerns) to highlight promising approaches to youth safety online.

As detailed in the [Social Media Platforms and Age-Appropriate Practices](#) section of this report, many platforms integrate age-specific features for users between the ages of 13 and 18 years old. These can include default privacy settings on accounts; app usage dashboards and settings; and restrictions for posting content, sending and receiving messages, accessing promoted and recommended content, and limiting screen time. In addition, parental controls and linked accounts can help assuage some parents' concerns by allowing them greater supervision and more decisions in their child's online experience.

While these features respond to current concerns about access to age-inappropriate material and the potentially addictive nature of technology, it is important to note their limitations. These features are not activated unless the associated account age is accurate. Additionally, parental controls place a high burden on parents, who do not always have the capacity, willingness, or digital skills to effectively use parental monitoring tools—which most do not even use.¹⁰⁵ When in use, increased surveillance of kids online may exacerbate digital abuse by allowing children and teens to be subjected to extreme monitoring and control over their online presence.¹⁰⁶ This could be particularly dangerous for LGBTQ+ youth, those seeking access to reproductive health care, or those experiencing sexual, physical, or emotional abuse at home.

When advocating for safer, healthier online spaces for youth, legislators and civil society should evaluate existing approaches to creating age-appropriate online environments and the associated risks to be addressed to highlight successful techniques that can be adopted across online operators.

4. Understand That Content-Based Restrictions Will Have Unintended Consequences for People from Vulnerable Communities

Content-based restrictions will face strict constitutional scrutiny and should be used sparingly to avoid allowing the politicization of content to drive mandates that change the nature of the internet and disproportionately impact vulnerable communities.

Much of age verification legislation stems from ongoing conversations about what information is appropriate or not appropriate for young people to access. While content-based restrictions will face strict constitutional scrutiny, any allowances to restrict speech in the name of protecting children can have far-reaching consequences for freedom of expression and access to information.

As legislators and courts determine the scope of age verification requirements, sensitive or politicized topics, like those surrounding gender, sexuality, race, and reproductive health care, may become targets to censorship or age-gating.¹⁰⁷ Allowing the politicization of content to drive age verification requirements can set a dangerous precedent for years to come, leaving users and companies responding to changing considerations of what is age-appropriate or not.

5. Invest in Cross-Sector Research and Collaboration to Create Standardized Best Practices and Protocols for Age Verification

More research is needed to fully understand the potential impacts of age verification and implementation. Insights from industry, civil society, regulators, and users of all ages should be taken into consideration to create standardized best practices and protocols for age verification.

Governments and societies should carefully consider how age verification may unintentionally impact users. Mandates will increase the frequency at which people are asked to provide government-issued identification to access online spaces and may desensitize users to requests for personal and sensitive information. Along with a lack of clarity about what constitutes age-appropriate material, this could lead to an increase in requests for age verification, even in online spaces in which identification is normally neither required nor needed, as

well as associated scams. Governments should play a role in determining the standard of verification and identification online, the role of digitized or digital IDs, and alternative age verification processes for people that lack traditional identification.

To further mitigate the negative impacts of age verification on users, cross-sector collaboration is needed to understand the full range of implications, develop best practices, and standardize protocols. This work is in progress at various stages.

The Digital Trust & Safety Partnership outlined **five guiding age assurance principles** and best practices that put user choice, safety, and needs at the forefront of age assurance practices. Google's recent **Legislative Framework to Protect Children and Teens Online** offers thoughtful considerations to improve youth experiences while minimizing user risk and ensuring oversight and accountability. Previous projects at the **International Organization for Standardization** and **Institute of Electrical and Electronics Engineers** could be revived to develop common technical standards for conducting and facilitating age verification at acceptable levels of efficacy, privacy, and security.

Cross-sector collaboration provides opportunities to include the perspectives of actors and users of all ages in crafting design approaches and legislation.

Appendix

Age Verification State Laws Passed in 2023

The table's terminology reflects language within the passed state bills.

Law	Status	Terminology	Targeted Online Operators and Scope	Age Verification Methods	Enforcement Mechanisms
Arkansas Act 612	Passed April 2023	"Reasonable age verification" include verifying that the person seeking to access the material is 18 years of age or older.	Commercial entities, including corporations, LLCs, partnerships, limited partnerships, and sole proprietorships that contain a substantial portion (>33.33%) of material harmful to minors.	- Digitized ID cards - Government-issued ID - Any commercially reasonable age verification method that holds an Identity Assurance Level 2 (IAL2)	Private lawsuits
Arkansas Act B89	Passed April 2023; Temporarily blocked by a U.S. District Court in August 2023	"Reasonable age verification" means to confirm that a person seeking to access a social media platform is at least 18 years old.	Social media platforms, defined by the bill as online forums that companies make available for account holders to create a public profile, establish an account, or register as a user for the primary purpose of interacting socially with other profiles and accounts, as well as upload/view other posts or interact with others. Social media platform does not include a social media platform that is controlled by a business entity that has generated less than \$100,000,000 in annual gross revenue in addition to other exceptions.	- A digitized ID card, including a digital copy of a driver's license - Government-issued ID - Any commercially reasonable age verification method	Attorney General enforcement, private lawsuits, and civil penalties
Connecticut SB3 - Public Act 23-56	Passed June 2023; Effective July 2024	Does not define age verification.	Social media platforms, including public or semi-public internet-based services or applications.	Does not enumerate acceptable age verification methods, as the law indirectly requires age verification	Attorney General enforcement
Louisiana HB 142	Passed June 2022; Effective January 2023	"Reasonable age verification methods" include verifying that the person seeking to access the material is 18 years of age or older.	Commercial entities, including corporations, LLCs, partnerships, limited partnerships, and sole proprietorships that contain a substantial portion (>33.33%) of material harmful to minors.	- Digitized ID card - Commercial age verification systems that use government-issued ID - Transactional data (e.g., mortgage, education, and employment records) to verify that the age of the user is 18 or older	Private lawsuits
Louisiana S162	Passed June 2023; Effective July 2024	"Commercially reasonable efforts to verify age ... with a level of certainty appropriate to the risks that arise from the information management practices" of Louisiana account holders to ensure minors, in this case an account holder reasonably believed or known to be under 16 and is not emancipated or married, do not hold an account without express consent of parent or guardian.	Social media companies with at least five million account holders worldwide and are considered an interactive computer service.	- Valid government-issued identity card - Completed parent/guardian consent form - A toll-free phone number for parent to consent via call - A video call with a minor's parent or guardian to obtain consent - Collecting government-issued identification of parent/ guardian - Consent via email and additional steps	Administrative fine, up to \$2,500, for each violation; civil penalties; and state lawsuits

Age Verification State Laws Passed in 2023

The table's terminology reflects language within the passed state bills.

Mississippi SB 2346	Passed April 2023	"Reasonable age verification" include verifying that the person seeking to access the material is 18 years of age or older.	Commercial entities, including corporations, LLCs, partnerships, limited partnerships, and sole proprietorships that contain a substantial portion (>33.33%) of material harmful to minors.	- Digitized ID card - Commercial age verification system that uses government-issued ID, or private transactional data to confirm user age	Private lawsuits
Montana S544	Passed May 2023	"Reasonable age verification methods" include verifying that the person seeking to access the material is 18 years of age or older.	Commercial entities, including corporations, LLCs, partnerships, limited partnerships, and sole proprietorships that contain a substantial portion (>33.33%) of material harmful to minors.	- Digitized ID card - Commercial age verification system that uses government-issued ID or private transactional data to confirm user age	Private lawsuits, punitive damages
North Carolina H8	Passed October 2023	Does not define age verification , but states age verification should be done through a commercially reasonable method.	Commercial entities, including corporations, LLCs, partnerships, limited partnerships, and sole proprietorships that contain a substantial portion (>33.33%) of material harmful to minors.	- A commercially available database that is regularly used by businesses or governmental entities for the purpose of age and identity verification - Another commercially reasonable method of age and identity verification	Civil liability damages, punitive damage, and private lawsuits
Texas HB18	Passed June 2023	Does not define age verification , but states "shall verify, using a commercially reasonable method." Age-gating is sufficient enough.	Digital service providers—defined as a website, application, program, or software that collects or processes personal identifying information with Internet connectivity and allows users to create public profiles, connect with other users, and create/post content.	Commercially reasonable method	Private lawsuits
Utah SB 152	Passed March 2023	Does not define age verification.	Social media companies, with at least five million account holders worldwide and considered an interactive computer service; account holders must be able to create profiles, upload/view other posts, and interact with others.	Does not enumerate acceptable age verification methods, but allows the Department of Commerce, Division of Consumer Protection to establish acceptable means, which may include a valid government-issued ID card	Private lawsuits, civil fines and penalties, administrative fines, and state action
Virginia SB1515	Passed May 2023	Does not define age verification.	Commercial entities and "interactive computer services," which means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the internet and such systems operated or services offered by libraries or educational institutions.	- A commercially available database that is regularly used by businesses or governmental entities for the purpose of age and identity verification - Another commercially reasonable method of age and identity verification, which can verify that any person attempting to access such material harmful to minors is 18 years of age or older	Civil liability damages

Arkansas Act 689 has extensive exceptions to what is considered a social media platform such that it mainly targets platform giants Instagram, Facebook, and X (formerly Twitter).

NEW AMERICA

Notes

- 1 Ayesha Rascoe and Saige Miller, “A New Utah Law Led Pornhub to Ban Access to Its Site for Everyone in the State,” NPR, May 7, 2023, <https://www.npr.org/2023/05/07/1174631536/a-new-utah-law-led-pornhub-to-ban-access-to-its-site-for-everyone-in-the-state>.
- 2 Rebecca Kern, “Big Tech carves loopholes out of state kids’ safety laws,” *POLITICO*, May 18, 2023, <https://www.politico.com/news/2023/05/18/tech-lobbyists-score-wins-in-state-kids-safety-laws-00096301>.
- 3 “Age Verification Bill Tracker,” Free Speech Coalition Action Center, 2024, <https://action.freespeechcoalition.com/age-verification-bills/>.
- 4 Monica Anderson and Michelle Faverio, “81% of U.S. adults – versus 46% of teens – favor parental consent for minors to use social media,” Pew Research Center, October 31, 2023, <https://www.pewresearch.org/short-reads/2023/10/31/81-of-us-adults-versus-46-of-teens-favor-parental-consent-for-minors-to-use-social-media/>; Donna St. George, “Schools sue social media companies over youth mental health crisis,” *Washington Post*, March 19, 2023, <https://www.washingtonpost.com/education/2023/03/19/school-lawsuits-social-media-mental-health/>; Cristiano Lima-Strong and Naomi Nix, “41 states sue Meta, claiming Instagram, Facebook are addictive, harm kids,” *Washington Post*, October 24, 2023, <https://www.washingtonpost.com/technology/2023/10/24/meta-lawsuit-facebook-instagram-children-mental-health/>.
- 5 Lee Tien, “After 10 Years, an Infamous Internet-Censorship Act is Finally Dead,” *Deeplinks* (blog), Electronic Frontier Foundation, January 21, 2009, <https://www.eff.org/deeplinks/2009/01/copa>.
- 6 Makena Kelley, “Child safety bills are reshaping the internet for everyone,” *The Verge*, August 29, 2023, <https://www.theverge.com/>
- 2023/8/29/23849375/kosa-child-safety-free-speech-louisiana-utah-parental-consent.
- 7 Eric N. Holmes, *Online Age Verification (Part I): Current Context* (Washington, DC: Congressional Research Service, 2023), <https://crsreports.congress.gov/product/pdf/LSB/LSB11020>.
- 8 *Age Assurance: Guiding Principles and Best Practices* (Washington, DC: Digital Trust & Safety Partnership, 2023), https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.
- 9 “Identity Verification,” in *Computer Security Resource Center Glossary*, National Institute of Standards and Technology, https://csrc.nist.gov/glossary/term/identity_verification.
- 10 “What is age verification?” Age Verification Providers Association, 2024, <https://avpassociation.com/consumerseu/>.
- 11 David L. Hudson, Jr., “Chilling Effect Overview,” Foundation for Individual Rights and Expression, <https://www.thefire.org/research-learn/chilling-effect-overview>.
- 12 *Child Online Protection Act of 1998*, Pub. L. NO. 105-277, 112 Stat.2631-736 (1998), *codified at* 47 U.S.C. § 231, <https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim>.
- 13 “Children’s Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business,” Federal Trade Commission, <https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business>.
- 14 “International Standards for Age Verification,” Age Verification Providers Association, <https://avpassociation.com/standards-for-age-verification/>; Paul A. Grassi, Michael E. Garcia, and James L. Fenton, *NIST Special Publication 800-63-3 Digital*

Identity Guidelines (Gaithersburg, MD: National Institute of Standards and Technology, June 2017), <https://pages.nist.gov/800-63-3/sp800-63-3.html>.

15 “LA HB142 | 2023 | Regular Session,” LegiScan, June 06, 2023, <https://legiscan.com/LA/bill/HB142/2023>.

16 “AR SB66 | 2023 | 94th General Assembly,” LegiScan, April 11, 2023, <https://legiscan.com/AR/bill/SB66/2023>; “MS SB2346 | 2023 | Regular Session,” LegiScan, April 18, 2023, <https://legiscan.com/MS/bill/SB2346/2023>; “MT SB544 | 2023 | Regular Session,” LegiScan, May 22, 2023, <https://legiscan.com/MT/bill/SB544/2023>; “NC H8 | 2023-2024 | Regular Session,” LegiScan, October 2, 2023, <https://legiscan.com/NC/bill/H8/2023>; “TX HB18 | 2023-2024 | 88th Legislature,” LegiScan, June 13, 2023, <https://legiscan.com/TX/bill/HB18/2023>; “VA SB1515 | 2023 | Regular Session,” LegiScan, May 12, 2023, <https://legiscan.com/VA/bill/SB1515/2023>.

17 “UT SB0152 | 2023 | General Session,” LegiScan, March 23, 2023, <https://legiscan.com/UT/bill/SB0152/2023>; “CT SB00003 | 2023 | General Assembly,” LegiScan, June 26, 2023, <https://legiscan.com/CT/bill/SB00003/2023>; “LA SB162 | 2023 | Regular Session,” LegiScan, June 28, 2023, <https://legiscan.com/LA/bill/SB162/2023>; “AR SB396 | 2023 | 94th General Assembly,” LegiScan, April 11, 2023, <https://legiscan.com/AR/bill/SB396/2023>.

18 Connecticut’s Act Concerning Online Privacy, Data and Safety Protections does not outright require age verification, but mandates: “No social media platform shall establish an account for a minor who is younger than 16 years of age unless the social media platform has obtained consent from the minor’s parent or legal guardian to establish such account.” With any violation of this law to be treated as an unfair trade practice, platforms may feel obligated to verify the ages of existing and new users to ensure compliance. See: *An Act Concerning Online Privacy, Data, and Safety Protections*, State of Connecticut General Assembly, 2023, <https://www.cga.ct.gov/2023/TOB/S/PDF/2023SB-00003-R02-SB.PDF>.

19 Ayesha Rascoe and Saige Miller, “A New Utah Law Led Pornhub to Ban Access to Its Site for Everyone in the State,” NPR, May 7, 2023, <https://www.npr.org/2023/05/07/1174631536/a-new-utah-law-led-pornhub-to-ban-access-to-its-site-for-everyone-in-the-state>.

20 Marc Novicoff, “A Simple Law Is Doing the Impossible. It’s Making the Online Porn Industry Retreat,” *POLITICO*, August 8, 2023, <https://www.politico.com/news/magazine/2023/08/08/age-law-online-porn-00110148>.

21 Hannah Natason, “Objection to sexual, LGBTQ content propels spike in book challenges,” *Washington Post*, June 9, 2023, <https://www.washingtonpost.com/education/2023/05/23/lgbtq-book-ban-challengers/>; Hannah Natason, “Half of challenged books return to schools. LGBTQ books are banned most,” *Washington Post*, December 23, 2023, <https://www.washingtonpost.com/education/2023/12/23/school-book-challenges-shelves-lgbtq-authors/>; “Defending Our Right to Learn,” American Civil Liberties Union, March 10, 2022, <https://www.aclu.org/news/free-speech/defending-our-right-to-learn>; John Villasenor, “Can a state block access to online information about abortion services?” Brookings Institution, July 27, 2022, <https://www.brookings.edu/articles/can-a-state-block-access-to-online-information-about-abortion-services>.

22 Lee Tien, “After 10 Years, an Infamous Internet-Censorship Act is Finally Dead,” *Deeplinks* (blog), Electronic Frontier Foundation, January 21, 2009, <https://www.eff.org/deeplinks/2009/01/copa>.

23 The *Digital 2024 Global Overview Report* found there were upwards of 5 billion social media user identities (equivalent to over 60 percent of the world’s population). In the United States, social media users’ identities are 71.3 percent of the total population. Note that user identities may not represent unique individuals. In addition, social media use will vary across demographics. See: *Digital / 2024 Global Overview Report* (New York: We Are

Social, 2024), <https://wearesocial.com/us/blog/2024/01/digital-2024-5-billion-social-media-users/>; and Jeffrey Gottfried, *Americans' Social Media Use* (Washington, DC: Pew Research Center, 2024), <https://www.pewresearch.org/internet/2024/01/31/americans-social-media-use/>.

24 See the Appendix for a breakdown of age verification legislation passed in 2023.

25 “TX HB18,” <https://legiscan.com/TX/bill/HB18/2023>.

26 “LA HB142,” <https://legiscan.com/LA/bill/HB142/2023>; “MS SB2346,” <https://legiscan.com/MS/bill/SB2346/2023>; “MT SB544,” <https://legiscan.com/MT/bill/SB544/2023>.

27 “NC H8,” <https://legiscan.com/NC/bill/H8/2023>; “TX HB18,” <https://legiscan.com/TX/bill/HB18/2023>; “UT SB0152,” <https://legiscan.com/UT/bill/SB0152/2023>.

28 “VA SB1515,” <https://legiscan.com/VA/bill/SB1515/2023>.

29 “LA HB142,” <https://legiscan.com/LA/bill/HB142/2023>; “MS SB2346,” <https://legiscan.com/MS/bill/SB2346/2023>; “MT SB544,” <https://legiscan.com/MT/bill/SB544/2023>; “NC H8,” <https://legiscan.com/NC/bill/H8/2023>; “AR SB66,” <https://legiscan.com/AR/bill/SB66/2023>.

30 “UT SB0152,” <https://legiscan.com/UT/bill/SB0152/2023>; “CT SB00003,” <https://legiscan.com/CT/bill/SB00003/2023>; “LA SB162,” <https://legiscan.com/LA/bill/SB162/2023>; “AR SB396,” <https://legiscan.com/AR/bill/SB396/2023>.

31 Arkansas Act 689 has extensive exceptions to what is considered a social media platform such that it mainly targets platform giants Instagram, Facebook, and X (formerly Twitter). See: Jess Weatherbed, “New Arkansas bill to keep minors off social media exempts most social media platforms,” *The Verge*, April 13, 2023, <https://www.theverge.com/2023/4/13/23681770/arkansas-social-media-bill-restricts-minors-parental-consent>.

32 “TX HB18,” <https://legiscan.com/TX/bill/HB18/2023>.

33 “CT SB00003,” <https://legiscan.com/CT/bill/SB00003/2023>; “AR SB66,” <https://legiscan.com/AR/bill/SB66/2023>.

34 “IN SB0017 | 2024 | Regular Session,” LegiScan, March 13, 2024, <https://legiscan.com/IN/bill/SB0017/2024>; “WY HB0078 | 2024 | Budget Session,” LegiScan, February 16, 2024, <https://legiscan.com/WY/bill/HB0078/2024>; “TN SB1792 | 2023-2024 | 113th General Assembly,” LegiScan, April 5, 2024, <https://legiscan.com/TN/bill/SB1792/2023>; “OH HB295 | 2023-2024 | 135th General Assembly,” LegiScan, October 24, 2023, <https://legiscan.com/OH/bill/HB295/2023>.

35 “State Age Verification Bill Moves Ahead with Amendment,” *Chicago Tribune*, January 16, 2024, <https://www.chicagotribune.com/2024/01/16/statehouse-age-verification-bill-moves-ahead-with-amendment/>; Cristiana Lima-Strong, “Arkansas law curbing kids’ social media access blocked for now,” *Washington Post*, August 31, 2023, <https://www.washingtonpost.com/technology/2023/08/31/arkansas-social-media-kids-blocked/>; Emma Bowman, “A Texas law requiring age verification on porn sites is unconstitutional, judge rules,” NPR, September 1, 2023, <https://www.npr.org/2023/09/01/1197380455/a-texas-law-requiring-age-verification-on-porn-sites-is-unconstitutional-judge-r>.

36 “CA AB2273 | 2021-2022 | Regular Session,” LegiScan, September 15, 2022, <https://legiscan.com/CA/bill/AB2273/2021>; Adi Robertson, “Gavin Newsom signs California social media overhaul for minors,” *The Verge*, September 15, 2022, <https://www.theverge.com/2022/9/15/23329654/california-governor-gavin-newsom-ab-2273-social-media-children-code-law-signed>.

37 Sam Metz, “Utah law requiring age verification for porn sites remains in effect after judge tosses lawsuit,” Associated Press, August 2, 2023, <https://apnews.com/article/porn-age-verification-lawsuit-dismissed-utah-23cf1851eeba6ca52ad3fdd0e846cb1f>; Kevin McGill, “Judge tosses challenge to Louisiana’s age verification law aimed at porn websites,” Associated Press, October 4, 2023, <https://apnews.com/article/porn-lawsuit-age-verification-louisiana-bbdf1afdc5c09feb104fe4199e20c22d>.

38 Brendan Pierson, “U.S. court upholds Texas law mandating age verification for online porn,” Reuters, March 8, 2024, <https://www.reuters.com/legal/us-court-upholds-texas-law-mandating-age-verification-online-porn-2024-03-08/>.

39 *Making Age-Verification Technology Uniform, Robust, and Effective Act*, S. 419, 118th Cong. (2023), <https://www.congress.gov/bill/118th-congress/senate-bill/419/text>; *Protecting Kids on Social Media Act*, S.1291, 118th Cong. (2023), <https://www.congress.gov/bill/118th-congress/senate-bill/1291>.

40 *Kids Online Safety Act*, S. 1409, 118th Cong. (2023), <https://www.congress.gov/bill/118th-congress/senate-bill/1409>.

41 Kat Tenbarge, “200 groups push Senate to vote on Kids Online Safety Act in 2024,” *NBC News*, December 6, 2023, <https://www.nbcnews.com/tech/social-media/kosa-kids-online-safety-act-speech-censor-rcna128249>.

42 Mathew Ingram, “Lawmakers are pushing an online safety bill for kids. Critics have free-speech concerns,” *Columbia Journal Review*, February 8, 2024, https://www.cjr.org/the_media_today/kosa_child_safety_online_zuckerberg_criticism.php.

43 Cristiano Lima-Strong, “Senate poised to pass biggest piece of tech regulation in decades,” *Washington Post*, February 15, 2024, <https://www.washingtonpost.com/technology/2024/02/15/kids-online-safety-act-kosa-senate/>; “Changes to

KOSA Are Improvements, but Congress Must Still Address Remaining Challenges With the Bill, Says OTI,” Open Technology Institute, February 16, 2024, <https://www.newamerica.org/oti/press-releases/changes-to-kosa-are-improvements-but-congress-must-still-address-remaining-challenges-with-the-bill-says-oti/>.

44 *Online Safety Act 2023*, (c. 50), United Kingdom Public General Acts (2023), https://www.legislation.gov.uk/ukpga/2023/50/pdfs/ukpga_20230050_en.pdf.

45 Chris Vallance and Tom Gerken, “Wikipedia will not perform Online Safety Bill age checks,” BBC, April 27, 2023, <https://www.bbc.com/news/technology-65388255>.

46 “Age Verification,” Australian Government eSafety Commissioner, <https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification>.

47 Josh Taylor, “Australia will not force adult websites to bring in age verification due to privacy and security concerns,” *The Guardian*, August 30, 2023, <https://www.theguardian.com/australia-news/2023/aug/31/roadmap-for-age-verification-online-pornographic-material-adult-websites-australia-law>.

48 “Online age verification: balancing privacy and the protection of minors,” Commission Nationale de l’Informatique et des Libertés, September 22, 2022, <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>.

49 “Making the Internet Age-Aware,” euCONSENT, <https://euconsent.eu/>.

50 “Online age verification: balancing privacy and the protection of minors,” Commission Nationale de l’Informatique et des Libertés, September 22, 2022, <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>.

51 Department of Infrastructure, Transport, Regional Development, Communications, and the Arts,

“Government response to the Roadmap for Age Verification,” Australian Government, August 2023, <https://www.infrastructure.gov.au/sites/default/files/documents/government-response-to-the-roadmap-for-age-verification-august2023.pdf>.

52 Josh Taylor, “Australia will not force adult websites to bring in age verification due to privacy and security concerns,” *The Guardian*, August 30, 2023, <https://www.theguardian.com/australia-news/2023/aug/31/roadmap-for-age-verification-online-pornographic-material-adult-websites-australia-law>.

53 Erica Finkle, “Bringing Age Verification to Facebook Dating,” Facebook, December 5, 2022, <https://about.fb.com/news/2022/12/facebook-dating-age-verification/>.

54 Ian Corby, “A summary of the achievements and lessons learned of the euCONSENT project and what comes next,” euCONSENT, December 7, 2022, <https://euconsent.eu/a-summary-of-the-achievements-and-lessons-learned-of-the-euconsent-project-and-what-comes-next/>.

55 See letter from Entertainment Software Rating Board, Yoti, and SuperAwesome to Federal Trade Commission: “RE: Application for Approval of a Verifiable Parental Consent Method Pursuant to the Children’s Online Privacy Protection Rule 16 C.F.R. §312.12(a),” Federal Trade Commission, June 2, 2023, https://www.ftc.gov/system/files/ftc_gov/pdf/Application-for-a-new-VPC-method-ESRB-SuperAwesome-Yoti-06-02-2023.pdf.

56 *Facial Age Estimation: White Paper* (London: Yoti, 2023), <https://www.yoti.com/blog/yoti-age-estimation-white-paper/>.

57 See, for example, “Comment from Center for Democracy & Technology,” Request for Comment Project No. P235402, Federal Trade Commission, August 21, 2023, <https://www.regulations.gov/comment/FTC-2023-0044-0350>.

58 “FTC Denies Application for New Parental Consent Mechanism Under COPPA,” Federal Trade Commission, March 29, 2024, <https://www.ftc.gov/news-events/news/press-releases/2024/03/ftc-denies-application-new-parental-consent-mechanism-under-coppa>.

59 *Facial Age Estimation: White Paper* (London: Yoti, 2023), <https://www.yoti.com/blog/yoti-age-estimation-white-paper/>.

60 Ayesha Rascoe and Saige Miller, “A New Utah Law Led Pornhub to Ban Access to Its Site for Everyone in the State,” NPR, May 7, 2023, <https://www.npr.org/2023/05/07/1174631536/a-new-utah-law-led-pornhub-to-ban-access-to-its-site-for-everyone-in-the-state>.

61 “Reno v. ACLU — Challenge to Censorship Provisions in the Communications Decency Act,” American Civil Liberties Union, June 20, 2017, <https://www.aclu.org/cases/reno-v-aclu-challenge-censorship-provisions-communications-decency-act>; “Ashcroft v. ACLU,” American Civil Liberties Union, June 29, 2004, <https://www.aclu.org/cases/ashcroft-v-aclu-0>.

62 Eric N. Holmes, *Online Age Verification (Part III): Current Context* (Washington, DC: Congressional Research Service, 2023), <https://crsreports.congress.gov/product/pdf/LSB/LSB11022>.

63 Stephanie Kunze, “Ginsberg v New York (1968),” Free Speech Center at Middle Tennessee State University, April 5, 2024, <https://firstamendment.mtsu.edu/article/ginsberg-v-new-york/>; Noah Feldman, “Sorry, Senators, But Kids Have Free Speech Rights Too,” *Washington Post*, April 27, 2023, https://www.washingtonpost.com/business/2023/04/27/social-media-ban-for-kids-under-13-isn-t-constitutional/569b8ec0-e4fe-11ed-9696-8e874fd710b8_story.html.

64 Michael J. Hanmer and Samuel B. Novey, *Who Lacked Photo ID in 2020?: An Exploration of the*

American National Election Studies (College Park, MD: Center for Democracy and Civic Engagement, 2023), https://www.voteriders.org/wp-content/uploads/2023/04/CDCE_VoteRiders_ANES2020Report_Spring2023.pdf.

65 *2021 FDIC National Survey of Unbanked and Underbanked Households* (Washington, DC: Federal Deposit Insurance Corporation, 2021), <https://www.fdic.gov/analysis/household-survey/2021execsum.pdf>.

66 Shoshana Weissmann, “Age-verification methods, in their current forms, threaten our First Amendment right to anonymity,” *Real Solutions* (blog), R Street, June 1, 2023, <https://www.rstreet.org/commentary/age-verification-methods-in-their-current-forms-threaten-our-first-amendment-right-to-anonymity/>.

67 Mark Keierleber, “Survey Reveals Extent that Cops Surveil Students Online — in School and at Home,” *The 74*, August 3, 2022, <https://www.the74million.org/article/survey-reveals-extent-that-cops-surveil-students-online-in-school-and-at-home/>.

68 “ID SB1253 | 2024 | Regular Session,” February 13, 2024, LegiScan, <https://legiscan.com/ID/bill/S1253/2024>; “TN SB2042 | 2023-2024 | 113th General Assembly,” LegiScan, March 12, 2024, <https://legiscan.com/TN/bill/SB2042/2023>.

69 Antigone Davis, “Parenting in a Digital World Is Hard. Congress Can Make It Easier,” *Meta*, November 15, 2023, <https://about.fb.com/news/2023/11/online-teen-safety-legislation-is-needed/>; Marc Novicoff, “A Simple Law Is Doing the Impossible. It’s Making the Online Porn Industry Retreat,” *POLITICO*, August 8, 2023, <https://www.politico.com/news/magazine/2023/08/08/age-law-online-porn-00110148>.

70 Marc Novicoff, “A Simple Law Is Doing the Impossible. It’s Making the Online Porn Industry

Retreat,” *POLITICO*, August 8, 2023, <https://www.politico.com/news/magazine/2023/08/08/age-law-online-porn-00110148>.

71 *More than just a number: How determining user age impacts startups* (Washington, DC: Engine, February 2024), <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/65d8b6ab876bfd5b70f8795e/1708701355604/FINAL+-+2024+More+Than+Just+A+Number.pdf>.

72 Shoshana Weissman and Canyon Brimhall, “Age-verification laws don’t exempt VPN traffic. But that traffic can’t always be detected,” *Real Solutions* (blog), R Street, August 29, 2023, <https://www.rstreet.org/commentary/age-verification-laws-dont-exempt-vpn-traffic-but-that-traffic-cant-always-be-detected/>.

73 Rita Liao, “China roundup: Tencent takes on sites trying to circumvent its age limits,” *TechCrunch*, September 11, 2021, <https://techcrunch.com/2021/09/11/china-roundup-tencent-takes-on-sites-trying-to-circumvent-its-age-limits/>.

74 Shan Li, “Game Changer: Tencent to Limit Playing Time, Verify IDs of Young Chinese,” *Wall Street Journal*, November 5, 2018, <https://www.wsj.com/articles/game-changer-tencent-to-limit-playing-time-verify-ids-of-young-chinese-1541418380>; Zhang Yangfei, “Tencent Games sues platforms over adult ID trade,” *China Daily*, August 9, 2021, <https://global.chinadaily.com.cn/a/202109/08/WS6137ff25a310efa1bd66e00e.html>.

75 Min-Jeong Lee, “South Korea Eases Rules On Kids’ Late Night Gaming,” *Wall Street Journal*, September 2, 2014, <https://www.wsj.com/articles/BL-KRTB-6517>.

76 “Ashcroft v. ACLU,” American Civil Liberties Union, June 29, 2004, <https://www.aclu.org/cases/ashcroft-v-aclu-0>.

77 Monica Anderson and Michelle Faverio, “81% of U.S. adults – versus 46% of teens – favor parental

consent for minors to use social media,” Pew Research Center, October 31, 2023, <https://www.pewresearch.org/short-reads/2023/10/31/81-of-us-adults-versus-46-of-teens-favor-parental-consent-for-minors-to-use-social-media/>; Donna St. George, “Schools sue social media companies over youth mental health crisis,” *Washington Post*, March 19, 2023, <https://www.washingtonpost.com/education/2023/03/19/school-lawsuits-social-media-mental-health/>; Cristiano Lima-Strong and Naomi Nix, “41 states sue Meta, claiming Instagram, Facebook are addictive, harm kids,” *Washington Post*, October 24, 2023, <https://www.washingtonpost.com/technology/2023/10/24/meta-lawsuit-facebook-instagram-children-mental-health/>.

78 *Health Advisory on Social Media Use in Adolescence* (Washington, DC: American Psychological Association, May 2023), <https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use>; Georgia Wells, Jeff Horwitz, and Deepa Seetharaman, “Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show,” *Wall Street Journal*, September 14, 2021, <https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739>; *Social Media and Youth Mental Health: U.S. Surgeon General Advisory* (Washington, DC: U.S. Department of Health and Human Services, 2023), <https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf>.

79 The social media strategies shared in this report are not a comprehensive view of all the strategies employed by social media platforms, but instead are intended to provide a snapshot of what popular social media platforms are doing to improve youth experiences online.

80 Sarah Perez, “TikTok CEO says company scans public videos to determine users’ ages,” *TechCrunch*, March 23, 2023, <https://techcrunch.com/2023/03/23/tiktok-ceo-says-company-scans-public-videos-to-determine-users-ages/>.

81 Pavni Diwanji, “How Do We Know Someone Is Old Enough to Use Our Apps?” Meta, July 27, 2021, <https://about.fb.com/news/2021/07/age-verification/>; Erica Finkle, Sheng Lou, Christine Agarwal, and Dave Fryer, “How Meta uses AI to better understand people’s ages on our platforms,” Meta, June 22, 2022, <https://tech.facebook.com/artificial-intelligence/2022/06/adult-classifier/>.

82 “Report a child under 13 on Instagram,” Instagram Help Center, <https://help.instagram.com/517920941588885>; “Report an Underage Child,” Facebook Help Center, <https://www.facebook.com/help/contact/209046679279097>.

83 Regarding age restriction rules, Google’s YouTube Official Blog states, “If our systems are unable to establish that a viewer is above the age of 18, we will request that they provide a valid ID or credit card to verify their age. We’ve built our age-verification process in keeping with Google’s Privacy and Security Principles.” However, Google does not detail what methods their systems use to establish a viewer’s age. See: The YouTube Team, “Using technology to more consistently apply age restrictions,” *YouTube Official Blog* (blog), Google, September 22, 2020, <https://blog.youtube/news-and-events/using-technology-more-consistently-apply-age-restrictions/>.

84 “Introducing New Ways to Verify Age on Instagram,” Meta, June 23, 2023, <https://about.fb.com/news/2022/06/new-ways-to-verify-age-on-instagram/>.

85 “Age ID Verification,” Roblox, <https://en.help.roblox.com/hc/en-us/articles/4407282410644-Age-ID-Verification>.

86 “Account Restrictions,” Roblox, <https://en.help.roblox.com/hc/en-us/articles/360000375686-Account-Restrictions>.

87 “Tools to help you achieve your own personal sense of digital wellbeing,” Google, <https://wellbeing.google/for-everyone/>; James Beser, “New

safety and digital wellbeing options for younger people on YouTube and YouTube Kids,” *Canada Blog* (blog), Google, August 10, 2021, <https://blog.google/intl/en-ca/company-news/technology/new-safety-and-digital-wellbeing/>.

88 “Ad-serving protections for teens,” Google Advertising Policies, <https://support.google.com/adspolicy/answer/12205906>.

89 “Safeguards for Teens,” Snapchat, <https://parents.snapchat.com/safeguards-for-teens>.

90 “Parents’ Ultimate Guide to TikTok,” Common Sense Media, December 14, 2022, <https://www.commonsensemedia.org/articles/parents-ultimate-guide-to-tiktok>.

91 Cormac Kennan, “New features for teens and families on TikTok,” TikTok, March 1, 2023, <https://newsroom.tiktok.com/en-us/new-features-for-teens-and-families-on-tiktok-us>.

92 “New Protections to Give Teens More Age-Appropriate Experiences on Our Apps,” Meta, January 9, 2024, <https://about.fb.com/news/2024/01/teen-protections-age-appropriate-experiences-on-our-apps/>.

93 “User safety,” TikTok, <https://support.tiktok.com/en/safety-hc/account-and-user-safety/user-safety>.

94 “Understand YouTube & YouTube Kids options for your child,” YouTube for Families Help, <https://support.google.com/youtubekids/answer/10495678>; “Filter or blur explicit results with SafeSearch,” Google Search Help, <https://support.google.com/websearch/answer/510>.

95 “Family Sharing. Share your favorite things with your favorite people,” Apple, <https://www.apple.com/family-sharing/>; “Set up parental controls with Family Sharing on iPhone,” iPhone User Guide, <https://support.apple.com/guide/iphone/set-up-parental-controls-iph00ba7d632/ios>.

96 “Tools and Resources for Parents,” Snapchat, <https://parents.snapchat.com/parental-controls>.

97 “Stay Connected With Your Teen Using Discord’s Family Center,” *Discord Blog* (blog), July 11, 2023, <https://discord.com/blog/discord-family-center-stay-connected-with-your-teen>.

98 “Giving Teens and Parents More Ways to Manage Their Time on Our Apps,” Meta, June 27, 2023, <https://about.fb.com/news/2023/06/parental-supervision-and-teen-time-management-on-metas-apps/>.

99 *Health Advisory on Social Media Use in Adolescence* (Washington, DC: American Psychological Association, May 2023), <https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use>.

100 Candice L. Odgers, “The great rewiring: is social media really behind an epidemic of teenage mental illness?” *Nature*, March 29, 2024, <https://www.nature.com/articles/d41586-024-00902-2>; danah boyd, “KOSA isn’t designed to help kids,” *Medium*, January 31, 2024, <https://zephoria.medium.com/kosa-isnt-designed-to-help-kids-335ab57cddae>.

101 Research for this report was completed prior to the unveiling of the American Privacy Rights Act, which would establish federal data privacy protections for Americans. The bill classifies data for users under the age of 17 as sensitive data, which could potentially lead online operators to institute age verification requests. See: House Committee on Energy and Commerce, “Committee Chairs Rodgers, Cantwell Unveil Historic Draft Comprehensive Data Privacy Legislation,” U.S. House of Representatives, April 7, 2024, <https://energycommerce.house.gov/posts/committee-chairs-rodgers-cantwell-unveil-historic-draft-comprehensive-data-privacy-legislation>.

102 “Online age verification: balancing privacy and the protection of minors,” Commission Nationale de l’Informatique et des Libertés, September 22, 2022,

<https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>.

103 Jérôme Gorin, Martin Biéri, and Côme Brocas, “Demonstration of a privacy-preserving age verification process,” Laboratoire d’Innovation Numérique de la Commission Nationale de l’Informatique et des Libertés, June 23, 2022, <https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process>.

104 Age Check Certification Scheme, “ISO Working Draft Age Assurance Systems Standard,” euCONSENT, November 2021, <https://euconsent.eu/download/iso-working-draft-age-assurance-systems-standard/>.

105 Naomi Nix, “Meta says its parental controls protect kids. But hardly anyone uses them,” *Washington Post*, January 30, 2024, <https://www.washingtonpost.com/technology/2024/01/30/parental-controls-tiktok-instagram-use/>.

106 “Types of Abuse,” National Domestic Violence Hotline, <https://www.thehotline.org/resources/types-of-abuse/>.

107 Hannah Natason, “Objection to sexual, LGBTQ content propels spike in book challenges,” *Washington Post*, June 9, 2023, <https://www.washingtonpost.com/education/2023/05/23/lgbtq-book-ban-challengers/>; Hannah Natason, “Half of challenged books return to schools. LGBTQ books are banned most,” *Washington Post*, December 23, 2023, <https://www.washingtonpost.com/education/2023/12/23/school-book-challenges-shelves-lgbtq-authors/>; “Defending Our Right to Learn,” American Civil Liberties Union, March 10, 2022, <https://www.aclu.org/news/free-speech/defending-our-right-to-learn>; John Villasenor, “Can a state block access to online information about abortion services?” Brookings Institution, July 27, 2022, <https://www.brookings.edu/articles/can-a-state-block-access-to-online-information-about-abortion-services>.



This report carries a Creative Commons Attribution 4.0 International license, which permits re-use of New America content when proper attribution is provided. This means you are free to share and adapt New America’s work, or include our content in derivative works, under the following conditions:

- **Attribution.** You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

For the full legal code of this Creative Commons license, please visit **creativecommons.org**.

If you have any questions about citing or reusing New America content, please visit **www.newamerica.org**.

All photos in this report are supplied by, and licensed to, **shutterstock.com** unless otherwise stated. Photos from federal government sources are used under section 105 of the Copyright Act.