Congressional Research Service
Informing the legislative debate since 1914

Identifying Minors Online

Updated June 10, 2024

Congressional Research Service
https://crsreports.congress.gov
R47884

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R47884

June 10, 2024

Clare Y. Cho
Specialist in Industrial Organization and Business Policy

Identifying Minors Online

Concerns about potential harms to minors on the internet, particularly on social media platforms, have grown in recent years. Dating to the 1990s, policymakers have enacted legislation seeking to protect minors online, some of which create requirements for entities that provide websites, mobile applications, and online platforms (collectively, website operators).

Website operators have developed various methods to determine users' ages, often in response to federal or state legislation. Some commonly used methods include (1) relying on self-identification, such as requiring a user to provide their date of birth or check a box to indicate the user is of a certain age; (2) requesting documentation, such as a photo identification (ID) or a digitized driver's license containing the user's name and age; and (3) using consumer data, such as analyzing user content posted on the website or an image of the user's face. Each of these age verification methods presents different advantages and challenges. For example, everyone can provide a date of birth, but a website operator cannot verify that information without additional data or documentation. A website operator that receives a user's government-issued photo ID might be assured that the individual meets a minimum age requirement, but not everyone has a government-issued photo ID. This might also raise consumer data privacy concerns, depending on how the information is shared and stored.

Some Members of Congress have proposed increasing protections for minors online by implementing additional requirements for website operators. Website operators might respond by (1) implementing changes for all users; (2) implementing changes for individuals identified as minors, potentially using one of the methods mentioned above; (3) no longer offering certain services; or (4) no longer offering the entire service in the United States.

If Congress chooses not to address age verification methods used by website operators in legislation, website operators might still develop and implement new age verification methods in response to public scrutiny, lawsuits, and laws enacted by states and other countries. If Congress wishes to address age verification in legislation, some potential options include the following:

- **Supporting research on age verification.** Congress could, for example, provide funding for or direct a federal agency to conduct research related to age verification. This might help inform Congress for future legislative action. Website operators would be able to continue using a wide range of age verification methods. The Kids Online Safety Act (H.R. 7891, S. 1409), for example, would direct some federal agencies to conduct a study evaluating methods to verify age at the device or operating system level.
- **Directing a federal agency to issue guidance or regulations.** An agency could, for example, provide criteria that are to be considered in the development of age verification methods. This could influence the age verification methods that website operators develop and use. A consideration might include how much authority to provide the agency. The Kids PRIVACY Act (H.R. 2801), for example, would direct the Federal Trade Commission to promulgate regulations requiring a risk-based approach to determine the age of a user.
- **Requiring or prohibiting certain age verification methods.** Website operators' responses would likely depend on the number and type of options specified. Allowing operators to use various forms of age verification, for example, might not address Congress's concerns or may raise new ones. Limiting the methods operators can use might increase the likelihood that they are unable or unwilling to determine a user's age. The Protecting Kids on Social Media Act (S. 1291), for example, would require social media platforms to take "reasonable steps beyond merely requiring attestation" and direct the Department of Commerce to establish a pilot program to provide secure digital identification credentials.
- **Implementing or supporting a government age verification system.** Legislative options could include directing a federal agency to develop a system to help confirm users' ages or incentivize states to implement an age verification system. Some considerations might include which agency would be best suited to provide the system and what information would be provided to whom.

Some general considerations for Congress might include (1) who should be responsible for determining an individual's age online, (2) how would legislation on age verification be implemented and what are the potential effects, and (3) how an entity conducting age verification online can confirm that individuals are who they claim to be.

Contents

Tables

Contacts

Concerns about potential harms to minors using the internet have grown over the last few years. Surveys conducted by the Centers for Disease Control and Prevention have found that the percentage of high school students considering suicide and experiencing persistent feelings of sadness increased over the last decade, particularly for females.[1] Some studies, including internal research conducted by website operators,[2] suggest that although some minors benefit from using social media, some minors are harmed.[3] The Biden Administration created an interagency task force on kids' online health and safety to "identify current and emerging risks of harm to minors associated with online platforms."[4]

Congress has enacted legislation seeking to protect minors online. Some of the legislation creates requirements for website operators:[5]

- The Children's Online Privacy Protection Act of 1998 (COPPA) requires operators of online services that collect personal information and that are directed to, or knowingly collect data from, children under 13 years of age to notify users about the data collection, obtain advance parental consent for the collection, and maintain "reasonable procedures" to protect the data.[6]
- The PROTECT Our Children Act of 2008 requires providers of electronic communication services and remote computing services to report information related to child sexual abuse material (CSAM) to the CyberTipline operated by the National Center for Missing and Exploited Children, which provides the information to law enforcement.[7] Providers are not required to monitor users and content or "affirmatively search, screen, or scan" for CSAM.[8]

[1] From 2011 to 2021, the percentage of high school students who seriously considered attempting suicide increased from 16% to 22% (19% to 30% for females, 13% to 14% for males), and the percentage who experienced persistent feelings of sadness or hopelessness increased from 28% to 42% (36% to 57% for females, 21% to 29% for males). See Centers for Disease Control and Prevention, *Youth Risk Behavior Survey: Data Summary and Trends Report, 2011-2021*, pp. 58-70, https://www.cdc.gov/healthyyouth/data/yrbs/yrbs_data_summary_and_trends.htm.

[2] This report uses the term *website* to refer to websites, online platforms, and mobile applications, and the term *website operator* for the entities that provide these websites.

[3] For example, see U.S. Surgeon General Vivek Murthy, *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory*, U.S. Department of Health and Human Services, 2023, https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf; Department of Science, Innovation, and Technology and Department of Digital, Culture, Media, and Sport, "Online Harms Research Publications: December 2022," U.K. Government, December 13, 2022, https://www.gov.uk/government/publications/online-harms-research-publications-december-2022; and Georgia Wells, Jeff Horwitz, and Deepa Seetharaman, "The Facebook Files: 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.

[4] White House, "Fact Sheet: Biden-Harris Administration Announces Actions to Protect Youth Mental Health, Safety, and Privacy Online," May 23, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/23/fact-sheet-biden-harris-administration-announces-actions-to-protect-youth-mental-health-safety-privacy-online/. The National Telecommunications and Information Administration (NTIA) published a request for public comment on behalf of the task force. See NTIA, "Initiative to Protect Youth Mental Health, Safety, and Privacy Online," 88 *Federal Register* 67733, October 2, 2023, https://www.federalregister.gov/documents/2023/10/02/2023-21606/initiative-to-protect-youth-mental-health-safety-and-privacy-online.

[5] An example of legislation Congress has enacted that does not create requirements for website operators is the Protecting Children in the 21st Century Act, which implemented a nationwide program to increase public awareness and provide education on strategies to promote safe use of the internet by children (P.L. 110-385, Title II, §§201-216; 15 U.S.C. §§6551-6555).

[6] P.L. 105-277, Division C, Title XIII, §§1301-1308; 15 U.S.C. §§6501-6506.

[7] P.L. 110-401, Title V, §§501-503 (has been amended twice: P.L. 115-395, P.L. 118-59); 18 U.S.C. §§2258A-2258E.

[8] Legislation requiring website operators to actively search for content might raise constitutional concerns under the (continued...)

Congress has held hearings and bills have been introduced proposing to increase protections for minors online by implementing additional requirements for website operators.[9] Several states have enacted laws creating requirements for websites that provide material intended for or likely to be accessed by minors and for websites that provide material that is deemed harmful to minors in the legislation.[10] Courts have ruled that some of these state laws likely violate the First Amendment.[11] In addition, some federal laws seeking to protect minors online have been deemed unconstitutional under the First Amendment by federal courts.[12]

A consideration for implementing requirements for website operators might include whether operators are able to identify minors. Some bills introduced in the 118th Congress and state laws require or would likely incentivize website operators to implement age verification methods.[13] This report discusses some methods used by website operators to determine users' ages and potential trade-offs associated with each method. It also analyzes selected legislative options to address age verification and provides some considerations for Congress related to age verification and protecting minors online.

Methods Used to Identify Minors Online

No federal statute explicitly requires website operators to determine the age of individuals who use their websites. Nevertheless, some website operators have developed age verification methods or use methods provided by third parties to prevent minors from accessing their websites,[14] often in response to federal and state laws. Some examples of age verification methods include the following:

Fourth Amendment. For more information, see CRS Legal Sidebar LSB10713, *The Fourth Amendment and the Internet: Legal Limits on Digital Searches for Child Sexual Abuse Material (CSAM)*, by Michael A. Foster.

[9] For example, see U.S. Congress, Senate Committee on the Judiciary, *Protecting Our Children Online*, hearing, 118th Cong., 1st sess., February 14, 2023, S. Hrg. 118-028 (Washington, DC: GPO, 2023), https://www.govinfo.gov/content/pkg/CHRG-118shrg52253/pdf/CHRG-118shrg52253.pdf.

[10] For example, see California Age-Appropriate Design Code (*California Civil Code*, Division 3, Part 4, Title 1.81.47, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.47.&part=4.&chapter=&article=); and Utah Social Media Regulation Act (*Utah Code*, Title 13, Chapter 63, https://le.utah.gov/xcode/Title13/Chapter63/13-63.html).

For an overview of some state laws seeking to protect minors online, see CRS Legal Sidebar LSB11020, *Online Age Verification (Part I): Current Context*, by Eric N. Holmes.

[11] For example, see CRS Legal Sidebar LSB11071, *NetChoice v. Bonta and First Amendment Limits on Protecting Children Online*, by Peter J. Benson; and Skye Witley, "Online Age-Check State Law Run into Constitutional Headwinds," *Bloomberg Law*, September 19, 2023, https://news.bloomberglaw.com/privacy-and-data-security/online-age-check-state-laws-run-into-constitutional-headwinds.

[12] For example, the Child Online Protection Act (P.L. 105-277, Division C, Title XIV, §§1401-1406; 47 U.S.C. §231). For more information, see CRS Report R47049, *Children and the Internet: Legal Considerations in Restricting Access to Content*, by Eric N. Holmes.

[13] Throughout this report, the term *age verification* is used to discuss all methods used to determine the age of an individual. The term *age assurance* is used as an umbrella term that includes *age verification* and *age estimation*, which consist of different methods (for example, see 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/). This report does not make this distinction.

[14] Examples of companies that offer age verification services include Onfido and Veratad. See Onfido, "Age Verification," 2023, https://onfido.com/use-cases/age-verification/; and Veratad Technologies, "Flexible, Secure Age Verification," 2023, https://veratad.com/solutions/age-verification/.

- Some websites associated with alcoholic beverages—such as Guinness, Budweiser, and Patron Tequila—require users to enter their birthdates to indicate that they are at least 21 years old before accessing content.[15]
- Instagram, a social media platform, requires users to enter their birthdate when creating an account to indicate that they are at least 13 years old; it provides different default settings for individuals ages 13-17.[16] Some users in certain countries also need to verify their age by (1) recording a video selfie that is shared with Yoti,[17] a company that uses artificial intelligence (AI) to conduct facial estimations, or (2) uploading certain forms of identification (ID), including a driver's license, passport, or birth certificate.[18]
- Tinder, a dating app, requires users to enter their birthdate when creating an account to indicate that they are at least 18 years old. It requires some users in certain countries to verify their age by providing a copy of their driver's license or passport; it does not allow users to verify their age with a resident card, temporary driver's license, or student ID.[19]
- Pornhub, a platform that hosts pornographic content, requires users in Louisiana to verify that they are at least 18 years old using a digital ID through the LA Wallet app.[20] Pornhub is blocking access for users in certain states in response to state laws.[21]

This section discusses potential trade-offs—such as level of assurance, feasibility for operators, accessibility for users, and user privacy—for some methods used to identify minors online. These methods are grouped into three categories: (1) users self-report their age or date of birth, (2) users provide documentation to verify their age, and (3) operators or third parties use data collected about individuals to determine their age.

Self-Identification or User Attestation

Some websites require users to self-attest that they meet a minimum age requirement—such as by checking a box or providing their age or date of birth—when creating an account or accessing the website. This age verification method can be accomplished by all individuals and generally requires relatively low effort and costs for operators. However, users can easily claim to meet the

[15] Guinness, https://www.guinness.com/en-us; Budweiser, https://us.budweiser.com/; and Patron Tequila, https://www.patrontequila.com/.

[16] Meta Platforms, "Introducing New Ways to Verify Age on Instagram," June 23, 2022, https://about.instagram.com/blog/announcements/new-ways-to-verify-age-on-instagram.

[17] Yoti, "Age Verification Should Be Just an Age," https://www.yoti.com/business/age-verification/.

[18] Instagram used to allow users to confirm their age with *social vouching* (i.e., other users confirm a user's age) but stated the option was removed to make improvements on October 13, 2022. Meta Platforms, "Introducing New Ways to Verify Age on Instagram," June 23, 2022, https://about.instagram.com/blog/announcements/new-ways-to-verify-age-on-instagram.

[19] Tinder, "How Does Age Verification Work?," https://www.help.tinder.com/hc/en-us/articles/360040592771-How-does-age-verification-work-.

[20] Adi Robertson, "Louisiana Now Requires a Government ID to Access Pornhub," *Verge*, January 3, 2023, https://www.theverge.com/2023/1/3/23537226/louisiana-pornhub-age-verification-law-government-id.

[21] Pornhub has restricted access in Arkansas, Mississippi, Montana, North Carolina, Utah, and Virginia (see Jon Brodkin, "Supreme Court Decides Not to Block Texas Law that Age-Gates Porn Websites," *ArsTechnica*, May 1, 2024, https://arstechnica.com/tech-policy/2024/05/supreme-court-lets-texas-keep-enforcing-age-verification-law-for-porn-sites/).

age requirement when they do not. A website operator cannot determine whether users are providing their actual age without additional information.

Documentation

Some websites require users to provide documentation to verify their age. These often include government-issued documents—such as a driver's license, passport, or birth certificate—or other documents that provide some combination of the individual's full name, photo, age, and date of birth, such as a medical record, school ID, or membership ID. A website operator has an incentive to accept a wide range of documents or documents that most individuals can access to increase the number of potential users. Some operators might choose not to accept certain documents to maintain a higher level of assurance.

The types of documents held by most individuals vary. For example, the number of valid passports in circulation suggests that the majority of U.S. citizens do not have a passport.[22] About 71% of individuals residing in the United States had a driver's license in 2022,[23] with over 90% of those ages 30-79.[24] About 1.3% of individuals ages 14 and 15 had a driver's license,[25] and the percentages of individuals ages 16, 17, and 18 that had a driver's license were about 25%, 43%, and 60%, respectively.[26] CRS could not find similar information for other state-issued IDs.

A larger number of minors have access to other documents, such as birth certificates and school IDs, but accessibility might remain an issue for some individuals. For example, although most individuals born in the United States have a birth certificate, about 14% of individuals in the United States in 2022 were born in a foreign country, some of which might not offer birth certificates.[27] While nearly all children under five in Western Europe and North America have a birth certificate, UNICEF estimates that 77% of children under five across the world have their

[22] In 2022, 151,814,305 valid passports were in circulation, according to U.S. Department of State, Bureau of Consular Affairs, "Reports and Statistics," https://travel.state.gov/content/travel/en/about-us/reports-and-statistics.html. That year, the number of U.S. citizens was 311,614,516, according to the Census Bureau's American Community Survey one-year estimates at U.S. Census Bureau, Table K200501: Citizenship Status in the United States, https://data.census.gov/table/ACSSE2022.K200501. This means that if each valid passport belonged to a different individual, at most, 48.7% of U.S. citizens had a U.S. passport. The actual percentage may be lower; an individual can have both a passport book and card, which counts as two valid passports, and qualifying non-U.S. citizens can have a U.S. passport.

[23] U.S. Department of Transportation (DOT), Federal Highway Administration (FHWA), Office of Highway Policy Information, Policy and Governmental Affairs, "6.3.1. Licensed Drivers—Ratio of Licensed Drivers to Population," *Highway Statistics Series 2022*, last modified on February 5, 2024, https://www.fhwa.dot.gov/policyinformation/statistics/2022/dl1c.cfm.

[24] DOT, FHWA, Office of Highway Policy Information, Policy and Governmental Affairs, "6.3.2. Licensed Drivers, by Sex and Percentage in Each Age Group (REVISED)," *Highway Statistics Series 2022*, last modified on May 6, 2024, https://www.fhwa.dot.gov/policyinformation/statistics/2022/dl20.cfm.

[25] The "under 16" group is compared with 14- and 15-year-old population estimates (ibid.). Ten states are estimated to have individuals younger than 16 with a driver's license in 2022 (see DOT, FHWA, Office of Highway Policy Information, Policy and Governmental Affairs, "6.3.3. Licensed Drivers, by State, Sex, and Age Group," *Highway Statistics Series 2022*, last modified on March 1, 2024, https://www.fhwa.dot.gov/policyinformation/statistics/2022/dl22.cfm).

[26] Ibid.

[27] In 2022, the number of foreign-born individuals (excluding U.S. citizens born abroad to American parent[s]) was 46,182,177, and the total U.S. population was 333,287,562, according to the Census Bureau's American Community Service one-year estimate (https://data.census.gov/table/ACSSE2022.K200503).

births registered, with 47% in the least developed countries.[28] Similarly, some schools might not offer a school ID, and some school IDs might not indicate the individual's birthdate or age.

Some documents might be considered more reliable and harder to falsify than others. For example, the REAL ID Act prohibits federal agencies from accepting drivers' licenses and state-issued IDs unless the cards meet certain standards;[29] enforcement is scheduled to begin on May 7, 2025.[30] In contrast, schools do not have a uniform ID system; there were 98,577 public schools, including kindergarten through high school, in the 2020-2021 school year.[31] Schools might implement different security standards, if any, and use various designs, styles, and formats that could make it difficult to determine which school IDs are legitimate and which are fake.

The ability to counterfeit or falsify documents would also depend on other factors, such as the systems used to share documents. For example, an image of a driver's license would likely be easier to alter than a digital version of a driver's license that is verified by a state agency, as discussed below in "Digital ID." Government-issued documents are considered to be reliable, and often used to verify an individual's identity. Sharing government-issued documents with other entities might raise greater privacy and identity theft concerns than sharing other types of documents.

Digital ID

Some states offer digital IDs in the form of a digitized driver's license and state ID (**Table 1**).[32] These digital IDs are accessible through an app operated by the state government or a company partnering with the state government, often with the state's Department of Motor Vehicles (DMV). Some states allow these digital IDs to be used only at Transportation Security Administration (TSA) PreCheck entrances at certain airports;[33] others allow various entities—such as restaurants, bars, credit unions, and websites—to accept digital IDs.

Most of the digital ID systems implemented by states thus far comply with standards set by two international organizations: the International Organization of Standardization (ISO) and the International Electrotechnical Commission (IEC).[34] The ISO/IEC 18013-5 standards provide technical and functional requirements to maintain security, privacy, and interoperability for mobile drivers' licenses.[35] These standards differ from the REAL ID requirements, which were

[28] UNICEF, "Birth Registration," last updated June 2023, https://data.unicef.org/topic/child-protection/birth-registration/.

[29] P.L. 109-13, Division B, Title II. For more information about REAL ID, see U.S. Department of Homeland Security (DHS), "About REAL ID," last updated May 7, 2024, https://www.dhs.gov/real-id/about-real-id.

[30] All states, the District of Columbia, and the five territories are REAL ID compliant. See DHS, "REAL ID Frequently Asked Questions," last updated August 30, 2023, https://www.dhs.gov/real-id/real-id-faqs.

[31] The number of private schools is reported every other year and was not reported for the 2020-2021 school year; there were 30,492 private schools in the 2019-2020 school year. See National Center for Education Statistics, "Educational Institutions," https://nces.ed.gov/fastfacts/display.asp?id=84.

[32] In this report, a *digital ID* refers to an electronic version of a government-issued document. It does not include other information individuals might use to identify themselves on the internet, such as usernames or sign-in information.

[33] For more information about using digital IDs at TSA PreCheck, see TSA, "Facial Recognition and Digital Identity Solutions," https://www.tsa.gov/digital-id.

[34] For example, see Utah Department of Public Safety, "Utah mDL FAQs," https://dld.utah.gov/mdlfaqs/; and Iowa Department of Transportation, "Iowa Mobile ID for Businesses, Organizations, and Agencies," https://iowadot.gov/mvd/MID-businesses.

[35] The International Organization of Standardization (ISO) and the International Electrotechnical Commission (IEC), *Personal Identification – ISO-compliant Driving License – Part 5: Mobile Driving License Application*, ISO/IEC 18013-5, September 2021.

expanded to mobile drivers' licenses in 2019.[36] The TSA has proposed rulemaking to temporarily waive the requirement that mobile drivers' licenses be compliant with REAL ID standards.[37] Digital IDs can be compliant with both ISO/IEC 18013-5 and REAL ID standards with some minor adjustments.[38]

Table 1. Selected Apps Providing Access to Digital IDs

State	Name of App	Operator of App[a]	Selected Places Accepting Digital ID	Website
Arizona	Apple Wallet	Apple	TSA	https://azdot.gov/apple-wallet
	Google Wallet	Google	TSA	https://azdot.gov/google-wallet
	Mobile ID	IDEMIA	N/A	https://azdot.gov/mvd/services/driver-services/mobile-id
	Samsung Wallet	Samsung	TSA	https://azdot.gov/samsung-wallet
California	CA DMV Wallet App*	California DMV	TSA, certain retail locations in Sacramento	https://www.dmv.ca.gov/portal/ca-dmv-wallet/
Colorado	Apple Wallet	Apple	TSA	https://dmv.colorado.gov/applewallet
	Google Wallet	Google	TSA	https://dmv.colorado.gov/colorado-id-in-google-wallet
	myColorado	Colorado Office of Information and Technology	Certain restaurants, bars, liquor stores	https://mycolorado.gov/colorado-digital-id
Delaware	Mobile ID	IDEMIA	N/A	https://www.dmv.de.gov/mobileID/
Florida	Smart ID*	Thales	N/A	https://www.flhsmv.gov/floridasmartid/
Georgia	Apple Wallet	Apple	TSA	https://dds.georgia.gov/ga-digital-drivers-license-and-id
	Google Wallet	Google	N/A	https://dds.georgia.gov/digital-id-google-wallet
Iowa	Mobile ID	IDEMIA	TSA, certain retail locations, restaurants, bars, credit unions	https://iowadot.gov/mvd/Mobile-ID
Louisiana	LA Wallet	Envoc	Certain retail locations, restaurants, bars, websites	https://lawallet.com/about/
Maryland	Apple Wallet	Apple	TSA	https://mva.maryland.gov/Pages/MDMobileID_Apple.aspx
	Google Wallet	Google	TSA	https://mva.maryland.gov/Pages/MDMobileID_Googlewallet.aspx

[36] P.L. 116-260, Division U, Title X, §1001.

[37] TSA, "Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Waiver for Mobile Driver's Licenses," 88 *Federal Register* 60056, August 30, 2023, https://www.federalregister.gov/documents/2023/08/30/2023-18582/minimum-standards-for-drivers-licenses-and-identification-cards-acceptable-by-federal-agencies-for.

[38] American Association of Motor Vehicle Administrators, *Mobile Driver's License (mDL) Implementation Guidelines*, version 1.2, January 2023, https://aamva.org/getmedia/b801da7b-5584-466c-8aeb-f230cef6dda5/mDL-Implementation-Guidelines-Version-1-2_final.pdf.

State	Name of App	Operator of App[a]	Selected Places Accepting Digital ID	Website
Mississippi	Mobile ID	IDEMIA	N/A	https://www.driverservicebureau.dps.ms.gov/mobile-id/
Utah	GET Mobile App	GET North America	TSA, certain credit unions, grocery stores, liquor stores	https://dld.utah.gov/utahmdl/

Source: CRS using information provided by state DMV websites and other websites.

Notes: TSA = Transportation Security Administration. An asterisk (*) indicates that the app is currently a pilot program with limited participants. N/A indicates that the website did not specify the places where the digital ID could be used.

a. If a company provides support for or continues to remain involved with the app, the company is listed as the operator. The company works with the state, which manages the program itself. The state's department is listed as the operator if it provides support for the app and is the listed entity in the app's terms of use.

Some of the accessibility concerns discussed in "Documentation" may be applicable to digital IDs. For example, because most individuals younger than 18 and nearly all individuals under 16 do not have a driver's license, a mobile driver's license would not be an option for most minors. However, the percentage of minors with a driver's license or other state-issued IDs might increase if these IDs can be used to access websites. Accessibility might remain an issue for some individuals if the app is provided only on mobile devices, particularly for individuals who do not have access to a mobile device and access the internet using computers and laptops.

A digital ID system might provide greater privacy protections than, for example, having individuals send photos of government-issued documents to every website they wish to access. A digital ID system could allow a government agency verify an individual's age without disclosing additional information to various website operators. Nevertheless, privacy concerns might depend on various factors, including the security of the system implemented and the amount and type of data the operator of a digital ID system would be able to access. There may be concern, for example, that the operator of the system would be able to track an individual's movements across websites. The operators of the digital ID systems mentioned in **Table 1** state that they do not store users' data.[39]

A potential complication with relying on digital IDs for age verification is that most states currently do not have a digital ID system that website operators can use to verify users' ages.[40] However, several states have implemented digital IDs for some entities, and other states might be implementing their own systems.[41] If states rely on companies to provide their digital IDs, it might raise concerns about potential unintended effects, such as whether consumers would be encouraged to use the companies' mobile wallets and other adjacent products.[42]

[39] For example, see IDEMIA, "Mobile ID: Frequently Asked Questions," https://na.idemia.com/dmv-2/mobile-id/.

[40] When this report was published, Louisiana was the only state that explicitly stated its digital ID system can be used for online identity verification (LA Wallet, "Bring Digital Verification to Your Business," https://lawallet.com/digital-verification/).

[41] For example, see Apple, "Apple Launches the First Driver's License and State ID in Wallet with Arizona," Apple Newsroom, last updated March 23, 2022, https://www.apple.com/newsroom/2022/03/apple-launches-the-first-drivers-license-and-state-id-in-wallet-with-arizona/; and Idemia, "Mobile ID: Everything Is on Your Phone. Now Your ID Is Too," https://na.idemia.com/dmv-2/mobile-id/.

[42] Grace Broadbent, "Samsung Wallet Adds State IDs to Compete Against Apple Pay and Google Pay," eMarketer, October 11, 2023, https://content-na1.emarketer.com/samsung-wallets-adds-state-ids-compete-against-apple-pay-google-pay.

Consumer Data

Consumer data can be used to estimate a user's age on a website. Data that might be used include conversations users have with their peers (e.g., upcoming birthday, classes), biometric data (e.g., image of a user's face), and data provided by other entities (e.g., credit card number).[43] Operators of websites that host large amounts of user-generated content may be able to use information provided directly on the website, while others might need to rely on data provided by other entities, such as data brokers, or age verification services offered by third parties.

To estimate a user's age, consumer data are typically analyzed using algorithms, AI, and other technologies; the accuracy depends on the system used. For example, some studies suggest that facial age estimation systems can estimate age within a range but have difficulty distinguishing between small differences in age (e.g., whether someone is 13 or 14 years old).[44] Additionally, the accuracy of these systems can be affected by factors such as facial expressions, makeup, color mode, and the use of props (e.g., glasses).[45] These systems might perpetuate or amplify biases in the datasets they are trained on.[46]

Using consumer data to estimate a user's age might raise privacy concerns. Website operators and third parties offering age verification services might be compelled to collect greater amounts of consumer data to develop and improve the models and systems used to estimate a user's age. For example, some methods of facial age estimation require large datasets.[47] Data collection and tracking tools—such as cookies and pixels—have enabled various entities to collect consumer data on the internet, which has led some policymakers to introduce or enact comprehensive consumer data privacy laws.[48]

Consumer data privacy laws might affect the feasibility of using consumer data for age verification. Comprehensive data privacy bills have been introduced in Congress,[49] and 18 states

[43] For example, see Lubna Takuri, "Age Verification System: How to Verify Customer Ages," Onfido, January 24, 2023, https://onfido.com/blog/age-verification-system/; Yoti, "Age Verification Should be Just an Age," https://www.yoti.com/business/age-verification/; and Google, "Access Age-Restricted Content and Features," Google Account Help, https://support.google.com/accounts/answer/10071085?hl=en.

[44] For example, Yoti reported that the probability that its facial age estimation system correctly identified an individual age 6-11 as younger than 13 was 98.35%. The results separated by skin tone and gender indicate that, on average, the system estimated the ages of individuals 6-11 within a range of 2.2 years or less (based on mean absolute error for each year). Yoti, *Yoti Facial Age Estimation*, white paper, March 2023, pp. 2, 5, https://www.yoti.com/wp-content/uploads/Yoti-Age-Estimation-White-Paper-March-2023.pdf.

[45] For example, see Prachi Punyani, Rashmi Gupta, and Ashwani Kumar, "Neural Networks for Facial Age Estimation: A Survey on Recent Advances," *Artificial Intelligence Review*, vol. 53 (2020), pp. 3299-3347, https://doi.org/10.1007/s10462-019-09765-w; and Tzvi Ganel, Carmel Sofer, and Melvyn Goodale, "Biases in Human Perception of Facial Age Are Present and More Exaggerated in Current AI Technology," *Nature: Scientific Reports*, vol. 12, no. 22519 (2022), https://www.nature.com/articles/s41598-022-27009-w.

[46] CRS Report R47644, *Artificial Intelligence: Overview, Recent Advances, and Considerations for the 118th Congress*, by Laurie A. Harris; and CRS Report R47569, *Generative Artificial Intelligence and Data Privacy: A Primer*, by Kristen E. Busch.

[47] For example, facial age estimation using convolutional neural network (CNN) frameworks require very large datasets for training; see Zichang Tan et al., "Efficient Group-n Encoding and Decoding for Facial Age Estimation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 40, no. 11 (2018), pp. 2610-2623, https://doi.org/10.1109/TPAMI.2017.2779808; and Oussama Guehairia et al., "Facial Age Estimation Using Tensor Based Subspace Learning and Deep Random Forests," *Information Sciences*, vol. 609 (September 2022), pp. 1309-1317, https://doi.org/10.1016/j.ins.2022.07.135.

[48] For more information, see CRS Report R47298, *Online Consumer Data Collection and Data Privacy*, by Clare Y. Cho and Kristen E. Busch.

[49] For example, a discussion draft of the American Privacy Rights Act (APRA) was passed by the Subcommittee on (continued...)

have passed comprehensive consumer data privacy laws; state laws in California, Colorado, Connecticut, Utah, and Virginia are currently enforceable (**Table 2**).

Table 2. Comprehensive Data Privacy Laws, by State

Name of State Law	Effective Date	Law Web Page
California Consumer Privacy Act[a]	January 1, 2020	https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5
Colorado Privacy Act	July 1, 2023	https://leg.colorado.gov/bills/sb21-190
Connecticut Data Privacy Act	July 1, 2023	https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB00006&which_year=2022
Delaware Personal Data Privacy Act	January 1, 2025	https://legiscan.com/DE/text/HB154/id/2807502/Delaware-2023-HB154-Draft.html
Indiana Consumer Data Protection Act	January 1, 2026	https://iga.in.gov/legislative/2023/bills/senate/5/details
Iowa Consumer Data Protection Act	January 1, 2025	https://www.legis.iowa.gov/docs/publications/LGE/90/SF262.pdf
Kentucky Consumer Data Protection Act	January 1, 2026	https://apps.legislature.ky.gov/record/24RS/hb15.html
Maryland Online Data Privacy Act	October 1, 2025	https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/sb0541
Minnesota Consumer Data Privacy Act	July 31, 2025	https://www.revisor.mn.gov/bills/bill.php?f=HF4757&b=house&y=2024&ssn=0
Montana Consumer Data Privacy Act	October 1, 2024	https://laws.leg.mt.gov/legprd/LAW0210W$BSIV.ActionQuery?P_BILL_NO1=384&P_BLTP_BILL_TYP_CD=SB&Z_ACTION=Find&P_SESS=20231
Nebraska Data Privacy Act	January 1, 2025	https://nebraskalegislature.gov/bills/view_bill.php?DocumentID=54904
New Hampshire	January 1, 2025	https://gencourt.state.nh.us/bill_status/billinfo.aspx?id=865&inflect=1
New Jersey	January 15, 2025	https://www.njleg.state.nj.us/bill-search/2022/S332
Oregon Consumer Privacy Act	July 1, 2024	https://olis.oregonlegislature.gov/liz/2023R1/Downloads/MeasureDocument/SB619/Enrolled
Tennessee Information Protection Act	July 1, 2025	http://www.capitol.tn.gov/Bills/113/Bill/SB0073.pdf
Texas Data Privacy and Security Act	July 1, 2024	https://capitol.texas.gov/BillLookup/Text.aspx?LegSess=88R&Bill=HB4
Utah Consumer Privacy Act	December 31, 2023	https://le.utah.gov/~2022/bills/static/SB0227.html
Virginia Consumer Data Protection Act	January 1, 2023	https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

Innovation, Data, and Commerce of the House Committee on Energy and Commerce on May 23, 2024 (markup available at https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=117372). For more information about APRA, see CRS Legal Sidebar LSB11161, *The American Privacy Rights Act*, by Chris D. Linebaugh et al.

Source: CRS using information compiled by the International Association of Privacy Professionals (IAPP). See Andrew Folks, "US State Privacy Legislation Tracker," IAPP, last updated May 28, 2024, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

Notes: The state is listed if the state law does not provide a common title. IAPP's U.S. State Privacy Legislation Tracker provides a chart identifying key provisions in the legislation. The list includes bills intended to be comprehensive approaches to govern the use of personal information; it does not include industry-specific, information-specific, or narrowly scoped bills (e.g., data security bills).

a. The California Consumer Privacy Act was amended by the California Privacy Rights Act, which was signed into law in 2020 and became fully operative on January 1, 2023.

The effect of data privacy laws might depend, in part, on how consumers respond. For example, all of the identified state comprehensive data privacy laws provide consumers with the right to delete their personal data and opt out of having their personal data collected for certain purposes. If enough consumers request their data to be deleted or not collected, these state laws might reduce the data that can be used for age verification. To reduce the burden on consumers, some companies and nonprofits have started offering services to send requests to companies to delete data on behalf of the consumer.[50] This, however, has raised concerns about the identity verification process used to ensure the data belong to the individual submitting the request.[51] Additionally, some states that do not have a comprehensive data privacy law have enacted legislation related to specific types of data, such as biometric data, that might affect the use of consumer data to conduct age verification (e.g., facial age estimation).[52]

Policy Considerations for Legislation

Multiple bills introduced in the 118th Congress seek to increase protections for minors online by creating requirements for website operators.[53] Some requirements for website operators, if included in enacted legislation, could be subject to constitutional challenges under the Free Speech Clause of the First Amendment.[54]

If Congress were to enact legislation creating requirements for website operators that are specific to minors, some operators might

- implement changes for all users;
- implement changes for individuals that the operator identifies as minors using one or more age verification methods, including those discussed in "Methods Used to Identify Minors Online";

[50] Kaveh Waddell, "How 'Authorized Agents' Plan to Make It Easier to Delete Your Online Data," *Consumer Reports*, March 21, 2022, https://www.consumerreports.org/electronics/privacy/authorized-agents-plan-to-make-it-easier-to-delete-your-data-a8655835448/; *Consumer Reports*, "Permission Slip: FAQ," https://permissionslipcr.com/faq.php; and Optery, "Removes Your Home Address, Phone and Other Private Info from Google and 270+ Sites," https://www.optery.com/.

[51] Kashmir Hill, "Want Your Personal Data? Hand Over More Please," *New York Times*, updated October 27, 2021, https://www.nytimes.com/2020/01/15/technology/data-privacy-law-access.html.

[52] For example, see Illinois General Assembly, Biometric Information Privacy Act, 740 ILCS 14/, https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57; and Washington State Legislature, Biometric Identifiers, Chapter 19.375, https://app.leg.wa.gov/RCW/default.aspx?cite=19.375.

[53] Some examples include the Kids Online Safety Act (S. 1409), Children and Teens' Online Privacy Protection Act (S. 1418), Social Media Child Protection Act (H.R. 821), Sammy's Law of 2023 (H.R. 5778), and EARN It Act of 2023 (H.R. 2732/S. 1207).

[54] For more information on potential constitutional concerns, see CRS Legal Sidebar LSB11021, *Online Age Verification (Part II): Constitutional Background*, by Eric N. Holmes; and CRS Legal Sidebar LSB11022, *Online Age Verification (Part III): Select Constitutional Issues*, by Eric N. Holmes.

- stop offering certain services (e.g., if websites were required to prevent adults from messaging minors, some websites might not allow any users or minors to communicate with other users); or
- stop offering the website. For example, some websites that primarily consist of pornographic content, including PornHub, have stopped offering their platform in certain states in response to state laws that require these websites to conduct age verification beyond self-declaration.[55] Some operators might try to avoid this option, particularly if their revenue comes primarily from the website.

The effectiveness of legislation might depend, in part, on the age verification methods used by the website operators. Although some website operators use various age verification methods, surveys and internal company data indicate that minors who are below the minimum age requirement continue to access some of these websites.[56] Each age verification method offers a different level of assurance and can raise various considerations, as discussed in the previous section. If Congress were not to enact legislation to increase protections for minors online, some website operators might still explore various safety measures and age verification methods in response to public scrutiny, lawsuits,[57] and laws enacted by states and other countries.[58]

This section analyzes some legislative options for addressing age verification. Specifically, this section provides some potential considerations if Congress chooses to (1) support research on age verification methods, (2) direct a federal agency to issue guidance or regulations specifying requirements related to age verification methods, (3) prohibit or require certain age verification methods, and/or (4) implement or support a government age verification system.

Support for Research

Congress has directed federal agencies to conduct research related to verifying identities online. Examples include the following:

- In 2019, the Government Accountability Office (GAO) analyzed online identity verification processes used by six federal agencies and whether they relied on information provided by consumer reporting agencies (e.g., Equifax, Experian,

[55] See footnote 21.

[56] For example, 38% of survey respondents ages 8-12 years old stated that they had used a social media platform in 2021 (see Common Sense, *The Common Sense Census: Media Use by Tweens and Teens*, March 9, 2022, https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens-2021). A chart from an internal presentation at Meta Platforms indicates that the monthly active people penetration was between 20% and 60% for individuals ages 11-13 who were born between 2000 and 2004, and an internal report estimated that 4 million U.S. individuals under 13 were on Instagram in 2015 (see "Complaint for Injunctive and Other Relief," *The People of the State of California et al. v. Meta Platforms, Inc.*, case no. 4:23-cv-05448-YGR (N.D. Cal), November 22, 2023, pp. 108-111).

[57] For example, multiple state attorneys general filed a lawsuit against Meta Platforms, Inc., for allegedly downplaying and concealing harms to minors caused by Facebook and Instagram, manipulating minors to spend more time on the platforms, and violating the Children's Online Privacy Protection Act of 1998 (COPPA). See "Complaint for Injunctive and Other Relief," *The People of the State of California et al. v. Meta Platforms, Inc.*, case no. 4:23-cv-05448-YGR (N.D. Cal), October 24, 2023, pp. 1-4.

[58] For example, see the U.K. Online Safety Bill and European Union's Digital Services Act at Department of Science, Innovation, and Technology and Department of Digital, Culture, Media, and Sport, "A Guide to the Online Safety Bill," U.K. Government, last updated August 30, 2023, https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill; and European Union, "Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)," October 27, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014.

and TransUnion),[59] as requested by Congress.[60] Two of the federal agencies no longer relied on information from consumer reporting agencies, and officials cited high costs and implementation challenges for not adopting alternative identify verification methods.

- In 2022, Congress directed the National Science Foundation (NSF), subject to the availability of appropriations, to provide awards to support research on distributed ledger technologies.[61] One of the listed potential research areas is the application of distributed ledger technologies for digital identities.[62] The legislation also allows the National Institute of Standards and Technology (NIST) to carry out a research project that would identify potential applications of distributed ledger technologies that could "improve the privacy and interoperability of digital identity and access management solutions."[63]

In the 118th Congress, legislation has been introduced to support research specifically on age verification methods. For example, the Kids Online Safety Act (H.R. 7891; S. 1409) would require certain federal agencies to "conduct a study evaluating the most technologically feasible methods and options for developing systems to verify age at the device or operating system level," in addition to implementing requirements that are unrelated to age verification for online platforms. Research on age verification methods might occur under broader proposals related to conducting research on online platforms. For example, the Platform Accountability and Transparency Act (S. 1876) would establish a research program for qualified researchers to access qualified data from certain online platforms if the research application is in the public interest, aims to study activity on a platform, and is used for noncommercial purposes.

Supporting research on age verification methods could help inform Congress, potentially for future legislative action. For example, a federal agency may be able to test the accuracy of some age verification methods and provide an in-depth analysis of potential benefits, harms, and risks. However, website operators would be able to continue using a wide range of age verification methods. Additionally, some researchers and organizations have published reports that examine some age verification methods and provide potential trade-offs.[64] Additional research might raise new considerations and legislative options.

Congressional considerations in this area might include who might need access to what types of data to provide information that would be helpful in creating federal legislation. For example, to create a comprehensive overview of potential age verification methods and their advantages and challenges, assembling a working group with researchers from industry, academia, and federal

[59] The Government Accountability Office (GAO) examined six federal agencies: Centers for Medicare and Medicaid Services, General Services Administration, Internal Revenue Service, Social Security Administration, U.S. Postal Service, and Department of Veterans Affairs. GAO, *Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes*, May 2019, https://www.gao.gov/assets/gao-19-288.pdf.

[60] The report specifies that congressional requesters included Senators Ron Wyden and Elizabeth Warren and Representatives Elijah E. Cummings and Jim Jordan (ibid., p. 39). Congress also requested a GAO report on consumer reporting agencies in the Economic Growth, Regulatory Relief, and Consumer Protection Act (P.L. 115-174), §308.

[61] P.L. 117-263, Division E, Title LIX, §5913; 42 U.S.C. §19222.

[62] Ibid., §(c)(1)(H)(i).

[63] Ibid., §(d)(2)(A)(i).

[64] For example, see Scott Brennen and Matt Perault, *Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?*, The Center for Growth and Opportunity, Utah State University, June 21, 2023, https://www.thecgo.org/research/keeping-kids-safe-online-how-should-policymakers-approach-age-verification/; and Shoshana Weissmann, "The Fundamental Problems with Social Media Age-Verification Legislation," R Street Institute, May 16, 2023, https://www.rstreet.org/commentary/the-fundamental-problems-with-social-media-age-verification-legislation/.

agencies might be sufficient. To analyze the number of minors accessing websites that rely on certain age verification methods, researchers may need access to these websites' internal, nonpublic data. This might raise additional considerations, such as how the internal data would be accessed and what information could be disclosed.

Requirements for Federal Agencies to Issue Guidance or Regulations

Congress has enacted legislation directing federal agencies to provide guidance or regulations related to verifying identities and protecting children's privacy online. Examples include the following:

- NIST provides guidance on identity verification standards for federal agencies that offer online services, such as login.gov,[65] through its *Digital Identity Guidelines*,[66] as required by the Federal Information Security Modernization Act of 2014.[67] The guidelines provide three levels of assurance within three main components: (1) enrollment and identity proofing, (2) authentication and lifecycle management, and (3) federation and assertions.[68] In May 2019, the Office of Management and Budget required federal agencies to implement NIST's *Digital Identity Guidelines*.[69]
- The FTC was directed to promulgate regulations for website operators under COPPA.[70] The FTC outlines steps companies can take to determine whether they are covered by COPPA,[71] provides information on how companies can comply with the law,[72] and has taken enforcement action against companies for violating the law.[73] On January 11, 2024, the FTC published a notice of proposed rulemaking to amend COPPA regulations. The notice seeks comments on various issues, including whether operators should be given an exception or other incentive to "conduct an analysis of their sites' or services' user bases" and

[65] Login.gov is currently compliant with the first identity assurance level (see General Services Administration, "Our Services," Login.gov Partners, https://www.login.gov/partners/our-services/). For more information about login.gov, see CRS In Focus IF12395, *Login.gov: Administration and Identity Authentication*, by Dominick A. Fiorentino, Natalie R. Ortiz, and Meghan M. Stuessy.

[66] Paul Grassi, Michael Garcia, and James Fenton, *Digital Identity Guidelines*, NIST Special Publication 800-63-3, last updated March 2, 2020, https://pages.nist.gov/800-63-3/. An initial public draft of the fourth revision is available at https://pages.nist.gov/800-63-4/.

[67] P.L. 113-283; 44 U.S.C. §§3551-3559.

[68] *Federation and assertions* refers to the protocol used in a federated environment to communicate authentication and attribute information, when applicable, to the party relying on this information. After the entity conducting the verification completes the authentication process, it generates an assertion containing the results to the requesting party. Ibid.

[69] Office of Management and Budget, "Memorandum for Heads of Executive Department and Agencies," May 21, 2019, https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf.

[70] 15 U.S.C. §6502.

[71] FTC, "Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business," https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business.

[72] Ibid. FTC, "Complying with COPPA: Frequently Asked Questions," https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.

[73] For a list of enforcement actions taken by the FTC, see FTC, "Cases Tagged with Children's Online Privacy Protection Act (COPPA)," https://www.ftc.gov/enforcement/cases-proceedings/terms/875.

examples of reliable methods operators can use to "determine the likely ages of a site's or service's users."[74] Operators are not required to determine users' ages.[75]

In the 118th Congress, legislation has been introduced to direct a federal agency to provide guidance or promulgate regulations. For example, the Kids PRIVACY Act (H.R. 2801) would direct the FTC to promulgate regulations requiring a risk-based approach to determine the age of a user, where higher privacy and security risks would require a higher certainty of the user's age. Some mandatory requirements could be subject to constitutional challenges.[76] Congress could also establish incentives for self-regulation by enabling industry groups and other entities to provide guidelines to meet regulations prescribed by a federal agency, similar to COPPA's safe harbor program.[77]

Guidance or regulations from a federal agency may influence the age verification methods that are developed and used by website operators. This could provide flexibility for website operators and other entities to explore new age verification methods, particularly if new options become feasible with technological developments, while addressing concerns some of the methods might raise. The effectiveness of agency guidelines or regulations would depend on the different criteria the guidelines or regulations would include and how feasible it would be for website operators to address. For example, if the regulations required a high level of assurance while prohibiting the use of government-issued documentation and consumer data, it might be difficult for website operators to comply.

The scope of the regulations may also arise as a consideration when issuing regulatory authority. For example, Congress could provide specific criteria that should be considered in the development of age verification methods and the importance of each, or it could allow an agency to determine what criteria should be considered. Providing more detail in legislation could provide greater clarity for companies, enforcers, and courts and help ensure the legislation is enforced as Congress intended. However, providing an agency with greater flexibility might allow the agency to respond to technological developments that make it feasible to implement new methods. This might also create some uncertainty, depending on how frequently agency-promulgated definitions or regulations are altered.

Requiring or Prohibiting Certain Age Verification Methods

Subject to the potential constitutional limitations mentioned above, Congress could require or prohibit website operators from using certain methods to determine a user's age. For example, the Protecting Kids on Social Media Act (S. 1291) would require social media platforms to take "reasonable steps beyond merely requiring attestation" and prohibit them from using or retaining "any information collected as part of the platform's age verification process." It would also direct the Department of Commerce to establish a pilot program to provide a secure digital identification credential for U.S. citizens and lawful residents. Legislation also could affect age

[74] FTC, "Children's Online Privacy Protection Rule," 89 *Federal Register* 2034, January 11, 2024, p. 2036, https://www.federalregister.gov/documents/2024/01/11/2023-28569/childrens-online-privacy-protection-rule.

[75] Ibid., p. 2037.

[76] CRS Legal Sidebar LSB11022, *Online Age Verification (Part III): Select Constitutional Issues*, by Eric N. Holmes.

[77] For more information about the safe harbor program, see FTC, "COPPA Safe Harbor Program," at https://www.ftc.gov/enforcement/coppa-safe-harbor-program.

verification methods indirectly. For example, legislation related to consumer data privacy or AI might incentivize operators to avoid certain age verification methods and rely on others.[78]

Website operators' responses to legislation prohibiting or requiring certain age verification methods would likely depend on the number of options specified and the legislative language used. For example, if legislation requires that operators use an age verification method other than a user's attestation, operators would have several methods to choose from. Similarly, certain terminology—such as requiring a "reasonable method of verification"—might be subject to interpretation and potentially result in a wide range of methods used.

Allowing website operators to use various age verification methods might result in different levels of assurance, privacy risks, and other trade-offs discussed in the section "Methods Used to Identify Minors Online." However, if legislation restricts operators to a limited number of age verification methods, it might increase the likelihood that operators are unable or unwilling to determine users' ages, particularly if the types of age verification methods allowed are costly and difficult to implement. It might increase the likelihood that website operators stop offering their services and might be more likely to raise constitutional concerns.[79]

Government Age Verification System

Congress has enacted legislation requiring federal agencies to use their records to confirm information provided by certain entities. Examples are as follows:

- In an effort to reduce fraud, Congress directed the Social Security Administration (SSA) to develop or modify a database to confirm the validity of certain personal information provided electronically by financial institutions if the individual gives consent.[80] In response, SSA created the electronic Consent Based Social Security Number Verification (eCBSV) service, which verifies that the individual's Social Security number (SSN), name, and date of birth combination matches SSA's records; it does not verify an individual's identity.[81]
- Congress directed the Attorney General to work with SSA and the Department of Homeland Security (DHS) to create a voluntary pilot program to compare information on employees' I-9 forms with government records to confirm each employee's identity and authorization to work in the United States.[82] The legislation states, "Nothing in this subtitle shall be construed to authorize, directly or indirectly, the issuance or use of national identification cards or the establishment of a national identification card."[83] The pilot program became E-

[78] For example, §6(a) of the Algorithmic Justice and Online Platform Transparency Act (H.R. 4624/S. 2325) would prohibit an online platform from using any proprietary design features that process personal information in a manner that makes certain goods or services unavailable based on biometric or other information. This might discourage website operators from using facial age estimation technologies to determine whether an individual can access the website.

[79] See the "Speech Rights of Website Operators" section in CRS Legal Sidebar LSB11022, *Online Age Verification (Part III): Select Constitutional Issues*, by Eric N. Holmes.

[80] P.L. 115-174, Title II, §215; 42 U.S.C. §405b.

[81] For more information, see Social Security Administration (SSA), "Information About eCBSV," https://www.ssa.gov/dataexchange/eCBSV/.

[82] P.L. 104-208, Title IV, Subtitle A, §§401-405; 8 U.S.C. §1324a note.

[83] P.L. 104-208, Title IV, Subtitle A, §404(h)(2).

Verify and is administered by DHS. Some states require some or all businesses to use E-Verify through contracting or business licensing laws.[84]

Legislative options could include expanding the entities that are able to use these services to include website operators or directing a federal agency to develop a new system to help confirm the age of users. Some considerations may include the following:

- **The level of assurance necessary to access a website.** Some websites might not need the same level of assurance as opening an account with a financial institution or confirming an employee's authorization to work in the United States. Congress might consider whether different websites need different levels of assurance and which age verification methods might be appropriate.
- **The federal agency best suited to provide an age verification system.** Some considerations might include what information the agency has access to, the agency's existing authorities, and whether the agency has the necessary resources and systems to provide the service.
- **What information would be provided and to whom.** Requiring individuals to provide their SSN to website operators, for example, might raise consumer privacy concerns, particularly as certain operators are not subject to the same consumer data protection requirements as other entities, such as financial institutions.[85] Additionally, if every website operator had to provide SSNs to SSA for verification, it might raise concerns about potential government surveillance. Another option could be providing individuals access to an age verification system, similar to how digital IDs are used to access certain websites in some states. Websites could direct individuals to log in to a system to obtain verification that the individual meets a certain age threshold without obtaining additional personal information. This option might not fully address concerns about government surveillance.
- **Whether operators and consumers would use the age verification system.** For example, the Dot Kids Implementation and Efficiency Act of 2002 directed the National Telecommunications and Information Administration (NTIA) to establish and oversee a second-level internet domain that would only provide access to material suitable for minors.[86] NTIA indefinitely suspended the second-level domain in 2012 because it was unable to gain public interest.[87] The effectiveness of an age verification system might depend, in part, on whether operators of popular websites use the system.

[84] For more information about E-Verify, see CRS Report R40446, *Electronic Employment Eligibility Verification*, by Andorra Bruno; DHS, "What Is E-Verify?," last updated June 2, 2023, https://www.e-verify.gov/about-e-verify/what-is-e-verify; and DHS, "History and Milestones," last updated May 4, 2023, https://www.e-verify.gov/about-e-verify/history-and-milestones.

[85] Financial institutions and their affiliates are subject to consumer data protection requirements under the Gramm-Leach-Bliley Act (15 U.S.C. §§6801-6809). For an overview of the Gramm-Leach-Bliley Act and other data protection laws, see CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh.

[86] P.L. 107-317; 47 U.S.C. §941.

[87] NTIA, ".us Domain Space," https://www.ntia.gov/page/us-domain-space (see "2007 Contract – Modification 0012" on June 27, 2012). According to an industry publication, the number of domain name registrations was relatively low, the use of the extension was limited, and it was determined that "there are now numerous websites with high-quality content aimed at children and numerous tools available to create a safe internet space for children." Hogan Lovells International LLP, "NTIA Suspends '.kids.us' Extension," *World Trademark Review Daily*, September 10, 2012, https://www.hoganlovells.com/-/media/hogan-lovells/pdf/publication/parlib011219512v1worldtrademarkreviewdailydtaylor100912_pdf.pdf.

- **Whether the legislation would raise concerns about federalism.** Many records of individuals—such as birth, marriage, and death records and drivers' licenses—are maintained by states, although some federal agencies and other entities acquire this information from states.[88] While Congress may be able to acquire or regulate this information in some circumstances, federalism principles may prevent Congress from mandating that states use the information to assist in federal age verification policies.[89]

Congress could also incentivize states to implement an age verification system, such as providing states with funding to assist with a system's development and implementation. For example, although states manage elections, the Help America Vote Act of 2002 implemented minimum standards for states and established the Election Assistance Commission to assist states with federal elections.[90] Congress could implement similar provisions for a digital ID system. Some states have implemented digital ID systems or are considering doing so, and providing incentives might encourage other states to implement systems that websites could use. It may be possible to implement similar systems with, for example, each state's division for vital records.[91]

Some states might not want to implement an age verification system, even if they are given incentives. A state digital ID system would raise some of the considerations mentioned above, such as which division would be best suited to provide information for an age verification system. A state-run system might raise additional considerations, such as whether there would be minimum standards or security levels across states and who would set these standards.

Concluding Observations

If Congress wishes to address age verification in legislation, some overarching considerations may include the following:

- **Who should be responsible for determining an individual's age online?** Requiring website operators to treat minors differently than adults without addressing age verification in legislation might place the responsibility of identifying users' ages on website operators. Some operators might be able to easily conduct age verification; others might not have the necessary resources to do so.
  A consideration may be what requirements, if any, should be placed on devices, intermediaries (e.g., app stores, web browsers), and state and federal agencies. For example, some intermediaries offer parental controls, and additional controls are offered by third-party subscription apps.[92] However, this scenario places the

[88] For example, the SSA acquires and maintains death data from states to administer some of its programs, and Naphsis, a nonprofit organization, provides access to birth and death data from most states. For more information, see CRS Report R46640, *The Social Security Administration's Death Data: In Brief*, by Paul S. Davies; and Naphsis, "Get Fast, Secure Access to Birth and Death Information," https://www.naphsis.org/get-vital-records/for-work/on-demand.

[89] For more information on federalism, see CRS Report R45323, *Federalism-Based Limitations on Congressional Power: An Overview*, coordinated by Kevin J. Hickey.

[90] P.L. 107-252; 52 U.S.C. §§20901-21145. For more information, see CRS In Focus IF12033, *The Help America Vote Act of 2002 (HAVA): An Overview*, by Karen L. Shanton.

[91] The vital records division in each state has birth, death, marriage, and divorce records. Contact information for the vital records division for each state is available at Centers for Disease Control and Prevention, National Center for Health Statistics, "Where to Write for Vital Records," https://www.cdc.gov/nchs/w2w/index.htm.

[92] For example, see Google, "How to Set Up Parental Controls on Google Play," Google Play Help, (continued...)

burden on guardians who might not be aware of the different parental controls available and their efficacy, as well as some of the risks associated with certain online platforms. Additionally, it might be difficult to implement these types of controls on devices used by multiple individuals, such as at libraries and schools.

- **How would legislation on age verification be implemented, and what are the potential effects?** For example, it would be less burdensome if users needed to verify their age once while creating an account with a website, rather than requiring users to verify their age every time they access a website. However, some websites currently do not require users to create an account. If legislation were to encourage users to create accounts with each website, it might increase the burden on users and potentially have indirect effects on the industry. For example, if individuals use the account information of popular platforms—such as Facebook, Google, and Apple—to access other websites, it might allow these companies to gather data that are not available for other operators.[93]
- **How can an entity conducting age verification online confirm that individuals are who they claim to be?** In person, a photo ID can be compared to the individual, which is not an option on the internet. Some websites use additional authentication methods—such as a security key, authentication app, or a link sent to a connected email address—to confirm individuals' identities when they create an account or access a website.[94] Some websites ask users to provide a selfie with specific requirements in the image so that the user needs to take a new photo at that moment.[95] Some minors may be able to bypass these security measures if, for example, they have access to their guardian's email address.

If Congress wishes to increase protections for minors online in legislation, some general considerations may include the following:

- **Whether requirements for website operators should address only minors.** Some content that may be considered harmful, such as online bullying and harassment, can affect all users.
- **Whether the legislation would apply to all websites or a subset.** Some policymakers have focused on websites that primarily host pornographic content and social media platforms. If certain types of content or services are associated with a greater risk of users being harmed, considerations may include how to define the platforms Congress wishes to address.[96]

---

https://support.google.com/googleplay/answer/1075738; Apple, "Use Parental Controls on Your Child's iPhone, iPad, and iPod Touch," November 1, 2023, https://support.apple.com/en-us/HT201304; Qustodio, https://www.qustodio.com/en/, and Net Nanny, https://www.netnanny.com/.

[93] For example, Pinterest allows users to sign in using Facebook and Google (see Pinterest, https://www.pinterest.com/), and Airbnb allows users to sign in using their Facebook, Google, and Apple account, as well as their email address or phone number (see Airbnb, https://www.airbnb.com/).

[94] For example, Login.gov requires additional authentication methods to create an account. See General Services Administration, "Create an Account," Login.gov, https://www.login.gov/create-an-account/. Using multiple authentication methods to access a website is also known as multifactor authentication or two-step verification; for more information, see Cybersecurity and Infrastructure Security Agency, "Multi-Factor Authentication," January 5, 2022, https://www.cisa.gov/resources-tools/resources/multi-factor-authentication-mfa.

[95] Kashmir Hill, "Want Your Personal Data? Hand Over More Please," *New York Times*, updated October 27, 2021, https://www.nytimes.com/2020/01/15/technology/data-privacy-law-access.html.

[96] For more information, see CRS Report R47662, *Defining and Regulating Online Platforms*, coordinated by Clare Y. Cho.

- **The feasibility of enforcing legislation.** For example, searches for virtual private networks (VPNs) reportedly spiked after some websites that primarily provide pornographic content stopped being offered in certain states in response to state age verification laws.[97]
- **Potential unintended effects.** For example, if legislation were to create requirements that are burdensome for platforms to implement, it might be difficult for nascent companies to enter and compete with incumbents that have more resources.

Author Information

Clare Y. Cho
Specialist in Industrial Organization and Business Policy

Acknowledgments

Lena Maman, Research Librarian, provided research assistance for this report.

Disclaimer

[97] Ned Oliver, "Virginia Leads Nation in VPN Searches After PornHub Block," *Axios*, July 7, 2023, https://www.axios.com/local/richmond/2023/07/07/pornhub-ban-virginia-vpn. A virtual private network (VPN) is a private network that can provide users with increased privacy, such as masking the IP address of their device so that the location of the device cannot be identified. For more information, see Sheila Frankel et al., *Guide to SSL VPNs: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-113, NIST, U.S. Department of Commerce, July 2008 pp. 6-36 and 6-37.