



# Challenges with Identifying Minors Online: A Brief Introduction

November 30, 2022

In the final weeks of the 117<sup>th</sup> Congress, [Members of Congress](#) are considering increasing protections for children online through the Kids Online Safety Act (S. 3663) and the Children and Teens' Online Privacy Protection Act (S. 1628). The bills would create requirements for operators of websites and mobile applications (apps), among other entities, to implement safeguards and other protections for minors. The U.S. Senate Committee on Commerce, Science, and Technology [approved both bills on July 27, 2022](#).

To protect minors online, Congress enacted the Children's Online Privacy Protection Act (COPPA; [15 U.S.C. §§6501-6506](#)) in 1998. COPPA requires operators of online services directed to children under 13 years of age that collect personal information to notify users about the data collection, receive parental consent, and maintain "reasonable procedures" to protect the data. Congress has enacted other legislation—such as the [Child Online Protection Act](#)—that federal courts have [deemed unconstitutional under the First Amendment](#).

## Current Efforts to Identify Minors

Some providers of online services have implemented minimum age requirements, typically stated in the providers' terms of service. Providers can use a minimum age requirement to assist them in complying with federal laws, such as COPPA, or to provide content that might not be suitable for minors.

To verify users' ages, many providers only require users to enter their birthdate or age before accessing the website or app, although some have set or are exploring additional requirements. For example, Tinder, a dating app, [requires users in some locations](#) to submit a copy of their driver's license, passport, or health insurance card to verify their age; it does not allow verification with a resident card, temporary driver's license, or student identification (ID) card. In June 2022, Instagram, a social media platform, started to [test three options for users to verify their age](#). Users can (1) record videos of themselves, which are shared with Yoti, a company that operates an [age-checking artificial intelligence \(AI\) technology](#); (2) ask other users to confirm their age; or (3) upload a driver's license or other [form of ID](#). In February 2021, Pornhub, a platform for pornographic content, [announced that only users verified with Yoti](#) would be able to upload content. On November 8, 2022, Anheuser-Busch, a beer brewing company, [launched a](#)

Congressional Research Service

<https://crsreports.congress.gov>

IN12055

responsible [delivery website](#) for retailers, including e-commerce, which [provides age verification recommendations](#).

## Potential Challenges with Identifying Minors

Providers of online services may face different challenges using photo ID to verify users' ages, depending on the type of ID used. For example, requiring a government-issued ID—such as a driver's license—might not be feasible for certain age groups, such as those younger than 13. In 2020, approximately [25% and 68% of individuals who were ages 16 and 19](#), respectively, had a driver's license. This suggests that most 16 year olds would not be able to use an online platform that required a driver's license. Other forms of photo ID, such as student IDs, could expand the age range with a photo ID. However, it may be easier to falsify a student ID than a driver's license. Schools do not have a uniform ID system, and there were [128,961 public and private schools](#)—including prekindergarten through high school—during the 2019-2020 school year, suggesting there could be various forms of IDs that could make it difficult to determine which ones are fake.

Another option could be creating a national digital ID for all individuals that includes age. Multiple states are exploring [digital IDs for individuals](#) by creating digital versions of a driver's license. Some firms are using [blockchain technologies](#) to identify users, such as for digital wallets and for individuals' health credentials. However, a uniform national digital ID system currently does not exist in the United States. Creating such a system could raise privacy and security concerns. Furthermore, it is unclear who would be responsible for creating and maintaining the system and verifying the information on it.

Several online service providers are relying on AI to identify users' ages. Thus, more firms have started to offer AI age verification services. For example, [Intellicheck](#) uses facial biometric data to validate an ID by matching it to the individual. However, commentators have raised concerns about [biases and the lack of transparency](#) with some of these AI technologies. For example, the accuracy of facial analysis software can depend on the [individual's gender, skin color, and other factors](#). Commentators have also [questioned the ability of AI software](#) to distinguish between small differences in age, particularly when individuals can use make-up and props to appear older.

Companies can also rely on data obtained directly from users or from other sources, such as [data brokers](#). For example, a company could [check a mobile phone's registration](#) information or analyze information on the user's social media account. However, this could raise data privacy and security concerns. Members of Congress have expressed concern about [online platforms' collection of consumer data](#).

## Policy Considerations for Congress

As Members of Congress consider implementing protections for minors, they may wish to consider potential unintended effects. For example, depending on the requirements of the legislation and severity of the penalties, legislation may create incentives for companies to collect more data on their users, limit availability of certain content for all users, and limit users who are able to access their platforms, including individuals who are not minors. Legislation that results in providers restricting access to content on their platforms may be subject to constitutional challenges in court under the Free Speech Clause of the First Amendment. If Congress chooses not to pursue legislative action, state laws—such as the [California Age-Appropriate Design Code Act](#)—and public scrutiny about harms to minors may incentivize providers of online services to implement new age verification requirements.

## Author Information

Clare Y. Cho  
Analyst in Industrial Organization and Business

---

## Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.