Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Challenges with Identifying Minors Online

Updated March 23, 2023

Congress has enacted legislation to protect minors online, such as the Children's Online Privacy Protection Act of 1998 (COPPA). COPPA requires operators of online services that collect personal information and are directed to, or knowingly collect, data on children under 13 years of age to notify users about the data collection, receive parental consent, and maintain "reasonable procedures" to protect that data. Congress has also enacted legislation—such as the Child Online Protection Act—that federal courts have deemed unconstitutional under the First Amendment.

Policymakers have shown interest in implementing additional protections for children on the internet. The Senate Judiciary Committee held a hearing, *Protecting Our Children Online*, on February 17, 2023. The 117th Congress introduced multiple bills—such as the Kids Online Safety Act and the Children and Teens' Online Privacy Protection Act—that would have created additional requirements for operators of online services. Some states have implemented legislation related to protecting children online, including California's Age-Appropriate Design Code Act and Louisiana's liability for publishers and distributors of material harmful to minors.

Current Efforts to Identify Minors

Federal statutes do not require providers of online services to use a specific method of age verification. Thus, some providers of online services have minimum age requirements—typically stated in the terms of service—and require users to enter their birthdate or age before accessing the content.

Some providers of online services have set or are exploring additional requirements to verify their users' ages. For example, the dating app Tinder 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, the social media platform Instagram 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, pornographic content platform Pornhub announced that only users verified with Yoti would be able to upload content. In January 2023, Pornhub started requiring users in Louisiana to verify their age with the LA Wallet app—a digital wallet that allows users to upload their driver's license, in addition to other information.

Congressional Research Service
https://crsreports.congress.gov
IN12055

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 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 age verification options. 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. 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 does not exist in the United States. Creating such a system could raise privacy and security concerns, and policymakers would need to determine who would be responsible for creating and maintaining the system, and verifying the information on it—responsibilities currently reserved to the states.

Several online service providers are relying on AI to identify users' ages, such as the services offered by Yoti, prompting firms to offer AI age verification services. For example, Intellicheck uses facial biometric data to validate an ID by matching it to the individual. However, AI technologies have raised concerns about potential biases and a lack of transparency. For example, the accuracy of facial analysis software can depend on the individual's gender, skin color, and other factors. Some 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 heighten data privacy concerns regarding online consumer data collection.

Policy Considerations for Congress

As Members of Congress consider implementing protections for minors, they may wish to consider potential unintended consequences. Depending on the requirements of the legislation and severity of the penalties, statutes may create different incentives for companies, such as collecting more data on users; limiting availability of certain content for all users; and limiting 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. State laws and public scrutiny about harms to minors may incentivize providers of online services to implement changes, regardless of congressional action. However, without federal legislation, providers may only implement changes for states that have passed laws without regard for the concerns of Congress.

Author Information

Clare Y. Cho
Analyst in Industrial Organization and Business

Disclaimer