Online age verification methods for children

Protecting children online is becoming increasingly vital. For over two decades, there has been a limited range of online age verification methods available to protect children from accessing online content unsuitable for their age. A number of countries are introducing legislation and/or codes of practice to address this situation. At EU level too, there are increasing efforts in this regard, with a code of practice in the pipeline. Challenges abound, however, in the areas of privacy, monitoring and the need to improve parents' and children's digital skills.

State of play

Children are very avid internet users; the coronavirus pandemic only amplified this trend, as children became used to spending more time online during the lockdowns. Global estimates reveal that one in three children is an internet user, and that one in three internet users is under 18. In the EU, most children use their smartphones daily, and almost twice as much as compared to 10 years ago. They also use them from a much younger age. More often than not, though, the online environments they access were not originally designed for them. Moreover, younger children have no problem bypassing the EU age requirements put in place by services such as social media, which require a minimum age of 13 for their users. One study found that digital services do not use adequate age verification or parental consent methods. This failing recently resulted in a record fine.

Main types of online age verification method

Online age verification methods are increasingly diverse. Below is a list of the most common ones.

- **Self-declaration**: this most common of all methods has been shown to be easily bypassed by children. Examples include self-declaring one's date of birth.
- **Credit card**: here, users are required to verify the validity of their cards, for instance, by making a bank or card payment of €0.01. This method is mostly used by e-commerce sites and apps selling adult products such as alcohol or adult content. Beyond the inherent risk of phishing, it is not possible to ascertain that the person using the card is the legitimate owner; moreover, the age for owning a credit card varies across countries.
- **Biometrics**: this method relies on artificial intelligence (AI), which powers the use of biometric technologies, including facial recognition applications. These may be used to analyse facial features with a selfie to ascertain that the individual requesting access is over 18. Establishing a person's age with accuracy is prone to errors; furthermore, underage individuals may use the face of someone older to gain unjustified access. What is more, authentication methods that use biometrics raise privacy issues because they may use special categories of personal data. Using applications to estimate a child's age can also lead to excessive data processing and to profiling.
- **Analysing online usage patterns**: this involves using age verification systems by inference, such as importing the individual's internet browsing history or analysing their 'maturity' by means of a questionnaire or their online user-generated content or purchases.
- **Offline verification**: this is done using scratch cards or offline in-situ age checks by means of documents.
- **Parental consent**: some apps and services require parental consent to register a child for a digital service. Yet, parental authority is rarely fully verified. Proving parental authority/guardianship might involve checking traditional identity (ID) documents and family registers.
- **Vouching**: this involves asking users other than the parents to vouch online as confirmation that a child seeking online access is of the right age.
- **Digital ID**: this method relies on tools offered by the state to verify individuals' identity and age before granting them access to digital services. For instance, China, Canada and Australia have

Author: Mar Negreiro, Members' Research Service
PE 739.350 – February 2023

introduced a digital ID for citizens. Some EU countries have also adopted this solution, and there is a proposal to create a European digital identity wallet.

- **Age verification by a specific app**: such apps are applied for a specific purpose. In France, for instance, users will soon have to install a government-licensed digital certification app to access online pornography content.

Only recently have social platforms started applying measures to verify age.

- In 2022, Instagram started testing a vouching tool to ensure users are as old as they say they are; it has also started using biometric technology for facial analysis in some cases.
- YouTube has launched a dedicated children's app and introduced new data practices.
- Meta has created Messenger Kids in Facebook that allows children to connect with parent-approved contacts only.
- Tiktok does not have an age-verification method but might ban accounts after sign-up.
- Twitter verifies parental consent requiring documentation (ID/birth certificate, etc.). Twitter says that the documents are treated confidentially and deleted after verification.
- e-Commerce sites selling adult products and services such as gambling, alcohol or pornography have a wide range of age verification methods such as credit and scratch cards and biometrics.

Main challenges and opportunities

A number of key challenges remain, of which the following three are particularly serious.

- **Privacy/cybersecurity concerns**: despite the widespread use of age verification methods in some sectors, there are still fears that they pose privacy and cybersecurity risks. Given the sensitivity of the data collected by some age verification systems, some suggest creating a specific trusted certification for third-party players. To date, there is no common EU guidance on methods for determining age verification; children easily bypass most solutions.
- **Content not attractive enough for children**: since children's apps and digital services tend to provide a limited set of functionalities, many children prefer to lie about their age to use the ones designed for adults. This makes children more vulnerable not only to privacy risks but also to safety threats, such as online grooming, or to exposure to content that is inappropriate for their age. There is a need to consider usability for young users during the software design phase.
- **Improved digital skills**: parents, children and guardians need better digital skills and a greater awareness of the risks involved. Some have also suggested that age verification should be an ongoing process that continues after sign-up.

What the EU is doing

Prior to the adoption of the General Data Protection Regulation (GDPR), which came into effect in 2018, there were no specific restrictions on the online processing of children's data in Europe. The GDPR requires the use of verification with regard to age and parental consent. Likewise, the Audiovisual Media Services Directive (AVMSD) requires the adoption of appropriate measures to protect children from online harmful content, including through age verification. In addition, the new European strategy for a better internet for children envisages a comprehensive EU code of conduct on age-appropriate design for 2024, building on the new rules in the Digital Services Act (DSA) and in line with the AVMSD and the GDPR. Such a code already exists in other parts of the world, such as the United Kingdom and California.

Moreover, in the context of the EU eID proposal, the Commission intends to strengthen age verification methods by means of a robust framework of certification and interoperability. In addition, the proposal for a regulation to combat child sexual abuse online envisages improved online age verification. There is also the EU co-funded euCONSENT project, which is building a browser-based interoperable age verification method. The European Parliament has called for better age verification methods to protect children online on several occasions, including in its own-initiative report on consumer protection in online video games adopted in January 2023 and its March 2021 resolution on children's rights in the light of the EU strategy on the rights of the child. Likewise, better age verification methods to protect children online are part of the European Commission's proposed European declaration on digital rights and principles for the digital decade and the OECD's Declaration on a Trusted, Sustainable and Inclusive Digital Future.