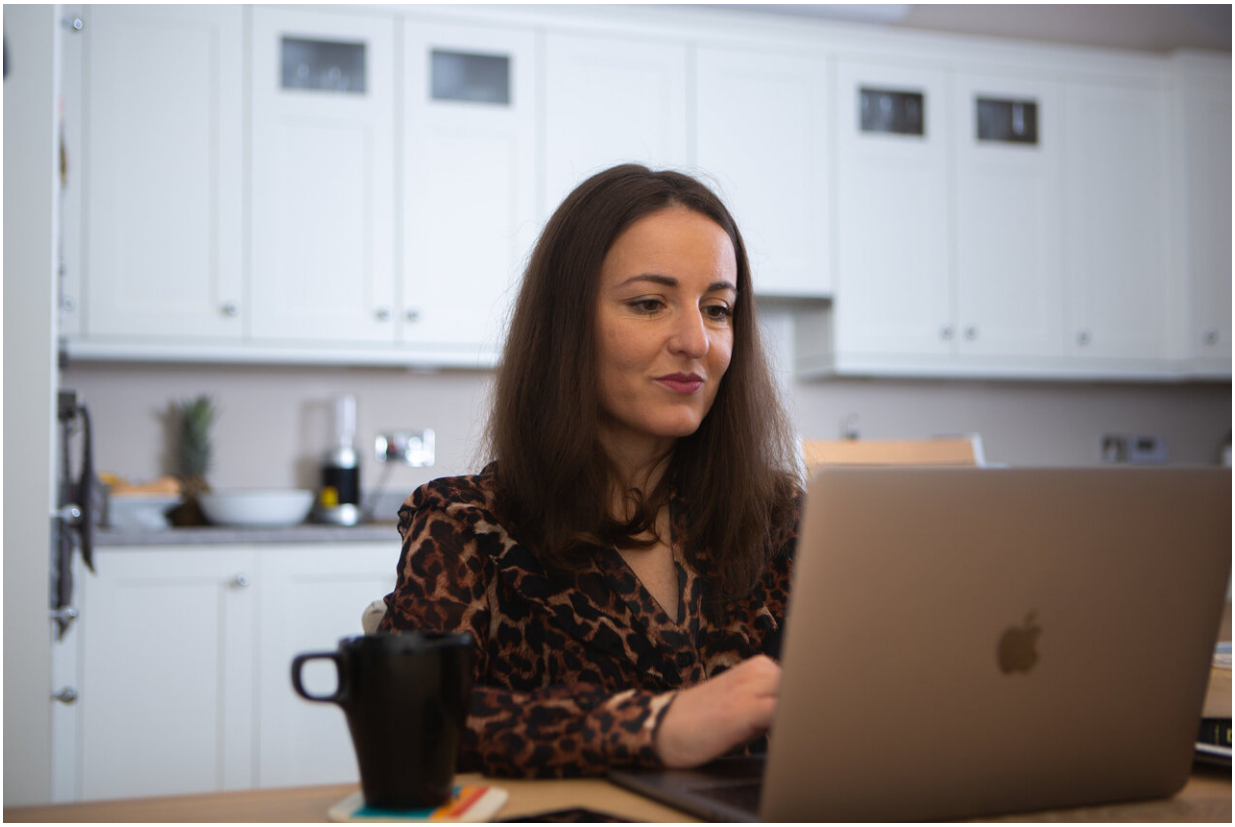
Children can bypass age verification procedures in popular social media apps

January 27 2021



Children of all ages can bypass age verification measures to sign-up to the world's most popular social media apps by simply lying about their age, a study led by Dr Liliana Pasquale of Lero, the Science Foundation Ireland Research Centre for Software at University College Dublin, Ireland has found. Credit: Piquant

Children of all ages can completely bypass age verification measures to sign-up to the world's most popular social media apps including Snapchat, Instagram, TikTok, Facebook, WhatsApp, Messenger, Skype and Discord by simply lying about their age, researchers at Lero, the Science Foundation Ireland Research Centre for Software have discovered.

And even potential age verification solutions identified by the research team can be easily sidestepped by children, according to the team's most recent study: Digital Age of Consent and Age Verification: Can They Protect Children?

Lead researcher Lero's Dr. Liliana Pasquale, assistant professor at University College Dublin's School of Computer Science, said children could easily bypass the mechanisms adopted by apps to verify their age.

"This results in children being exposed to privacy and safety threats such as cyberbullying, online grooming, or exposure to content that may be inappropriate for their age," she added.

The study which examined Snapchat, Instagram, TikTok, HouseParty, Facebook, WhatsApp, Viber, Messenger, Skype, Discord apps scrutinised age verification procedures in April 2019 and repeated it in April 2020—it found all ten apps permitted users, regardless of age, to set up accounts if they first gave their age as 16.

Dr. Pasquale said the widespread use of age of 13 as the minimum age for accessing social media services derives from the Children's Online Privacy Protection Act (COPPA), effective in the U.S. since 2000. Europe's General Data Protection Regulation (GDPR) requires children below the age of digital consent (13-16) to have verifiable parental consent for the processing of their data.

EU member states are also free to set a different digital age of consent, between 13 and 16 years, leading to a range of age limits across Europe. For example, Ireland, France, Germany and The Netherlands have opted for 16, while Italy and Spain have set the age at 14; while the UK, Denmark, and Sweden have set the age at 13.

"Our study found that while some apps disabled registration if users input ages below 13, but if the age 16 is provided as input initially then none of the apps require a proof of age. Providing mechanisms that deter a user from installing an app on a device on which they have previously declared themselves to be underage is currently one of the most sensible solutions not to incentivise users to lie about their age," Dr. Pasquale said.

The team looked at existing age recognition techniques using biometrics such as speech recognition and fingerprint characteristics as possible solutions to implement more robust age verification mechanisms. However, these were also found to have limitations with speech recognition, for example, easily bypassed by playing voice recordings.

Dr. Pasquale said their study found existing data protection regulations to be ineffective.

"In reality, the application of substantial financial penalties was the main trigger for app providers to implement more effective age verification mechanisms. Based on our study and on our survey of biometrics-based age recognition techniques, we propose a number of recommendations to app providers and developers," she said.

Recommendations:

- Clarify the minimum age and treatment of data: Existing apps should ensure that a clear, concise and age-appropriate summary

of the relevant parts of the app's ToU (terms of use) is displayed to users who sign-up and declare their age to be under 18.

- Enable the most restrictive privacy settings: Apps should apply the most restrictive privacy settings by default for any user that declares themselves to be under the age of 18. For example, photos, posts and messages should only be shared with "friends", location data should not be collected at all. It should also not be possible to override privacy settings without explicit parental consent.
- Encourage users not to lie about their age: Despite the presence of a minimum age requirement, many underage users continue to use social and communication apps. Users must be incentivised to be honest about their age, with minimal data collected. Providing mechanisms that deter a user from installing an app on a device on which they have previously declared themselves to be underage is currently the most sensible solution and the hardest to circumvent.
- Implement Robust Age Verification Mechanisms: Where a minimum age requirement is in place, it should be backed up by appropriate age verification mechanisms. Using age recognition techniques based on biometrics factors, such as facial features, may not be sufficient considering that these can be circumvented. Age verification should be an ongoing process that does not terminate after sign-up, to assess whether a user lied about his/her age at the moment of sign-up, to counteract evasion measures.

More information: Liliana Pasquale et al, Digital Age of Consent and Age Verification: Can They Protect Children?, *IEEE Software* (2020). DOI: 10.1109/MS.2020.3044872

Provided by Lero