Repository Istituzionale dei Prodotti della Ricerca del Politecnico di Bari

Digital Age of Consent and Age Verification: Can They Protect Children?

This is a post print of the following article

Original Citation:
Digital Age of Consent and Age Verification: Can They Protect Children? / Pasquale, Liliana; Zippo, Paola; Curley, Cliona; O'Neill, Brian; Mongiello, Marina. - In: IEEE SOFTWARE. - ISSN 0740-7459. - STAMPA. - 39:3(2022), pp. 50-57. [10.1109/MS.2020.3044872]

Availability:
This version is available at http://hdl.handle.net/11589/224464 since: 2023-05-22

Published version
DOI:10.1109/MS.2020.3044872

Publisher:

Terms of use:

(Article begins on next page)

02 January 2025

Department: Head
Editor: Name, xxxx@email

Digital Age of Consent and Age Verification: Can They Protect Children?

Liliana Pasquale
University College Dublin and Lero, Ireland

Paola Zippo
Politecnico di Bari, Italy

Cliona Curley
University College Dublin, Ireland

Brian O'Neill
Technological University Dublin, Ireland

Marina Mongiello
Politecnico di Bari, Italy

***Abstract*—Children are increasingly accessing social media content through mobile devices. Existing data protection regulations have focused on defining the digital age of consent, in order to limit collection of children's personal data by organizations. However, children can easily bypass the mechanisms adopted by apps to verify their age, and thereby be exposed to privacy and safety threats. We conducted a study to identify how the top 10 social and communication apps among underage users apply age limits in their Terms of Use. We also assess the robustness of the mechanisms these apps put in place to verify the age of their users. Moreover, we discuss how automated age recognition techniques can be adopted to increase the effectiveness of the age verification process. Finally, we provide recommendations to app providers and developers to specify the Terms of Use and implement robust age verification mechanisms.**

INTRODUCTION The widespread adoption of smartphones and tablets has allowed even small children to use mobile apps. A report [1] describing children's use of social media between 2015 and 2019 has indicated that, by the age of 3-4, children often access online content unsupervised by an adult. By the age of 15, about 89% of the children surveyed had a social media profile. There are different reasons inducing a child to have a social media profile, such as chatting with

 Published by the IEEE Computer Society © 2019 IEEE

friends, seeking new virtual friends, or increasing popularity by publishing pictures and videos.

Existing data protection regulations, such as the Children's Online Data Protection Act (COPPA) in the USA and the General Data Protection Regulation (GDPR) in Europe, have mainly focused on regulating collection of children's personal data. They have defined the concept of *digital age of consent*, i.e. the minimum age a user must be before organizations can collect, process and store their data without parental consent. Users under this age are referred to as underage users. The GDPR also requires the controller to verify that consent is given by the holder of parental responsibility over the child. However, some apps do not even ask for the age of their users during sign-up. Even when they do so, they provide very limited mechanisms to verify that a user is inputting his/her real age. As a result, children can easily bypass the mechanisms adopted by apps to verify the age of the user [5].

In some instances, providers have created alternative versions of their apps for kids. For example, Messenger Kids — the Facebook Messenger version for children — only allows children to connect with parent-approved contacts and does not allow deletion of messages. SnapKidz — the Snapchat version for children under 13 — lets users take, edit and store pictures locally, but it does not allow sending and receiving snaps. Because these apps only provide a limited set of functionalities, children prefer to lie about their age, in order to use apps originally designed for adults. This makes children more vulnerable to privacy and even safety threats [3], such as cyberbullying, online grooming, or exposure to content that may be inappropriate for their age.

Very few approaches (e.g. [4]) have considered underage users during the software engineering process. As far as we are aware, this is the first work to assess whether the laws regulating the digital age of consent and the age verification mechanisms implemented by apps can protect underage users. In this paper we provide a brief overview of the COPPA and the GDPR provisions about the digital age of consent. We subsequently report on a study aimed to review the top 10 social and communication apps used by children in 2019 and 2020. We assess how these apps implement age limits in their Terms of Use and what mechanisms they put in place to verify the age of their users. Moreover, we review existing biometrics-based age recognition techniques to assess whether and how they can be used to improve robustness of the age verification process. We conclude the paper by providing a set of recommendations to app providers and developers.

DIGITAL AGE OF CONSENT

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 USA since 2000. Digital service providers are obliged to acquire verifiable parental consent for children under the age of 13, who may use their service. Means of supplying parental consent include electronic scans, parental payment systems, video or phone conference, or through the use of government-issued IDs. Due to the costs and complexity involved, many service providers choose not to allow children to use such services by restricting access via their terms of use to those over the age of 13.

Prior to the European General Data Protection Regulation (GDPR), which came into effect in 2018, there were no specific restrictions on the processing of children's data in Europe. Under Article 8, GDPR requires children below the age of digital consent (13-16) to have verifiable parental consent for the processing of their data. Enhanced data protection for children by design and by default (Article 23) is therefore one of the key measures contained within GDPR. EU member states are also free to set a different digital age of consent, between 13 and 16 years, thus leading to a more complex range of age limits that apply across Europe. For example, Ireland, France, The Netherlands, and Germany have opted for 16, while Italy and Spain have set the age to 14; while the UK, Denmark, and Sweden have set the age at 13.

In contrast to COPPA which has quite specific requirements and conditions, the GDPR does not specify how parental consent should be obtained, nor does it oblige service providers to obtain any additional verification of age once users register, truthfully or otherwise, to access their service. In practice, such restrictions are likely to come

from codes of conduct which the GDPR encourages member states and supervisory authorities to develop. In the meantime, most service providers have responded by limiting the nature and amount of data they collect from users under the digital age of consent, while continuing to place the main emphasis on restricting access to under-13s in order to avoid infringing COPPA regulations.

TERMS OF USE AND AGE VERIFICATION

We evaluated how social and communication apps implement age limits in their Terms of Use (ToU) and what mechanisms they put in place to verify the age of their users. We addressed the following research questions (RQs):

1) Do the ToU of social and communication apps take into account the age limits prescribed by existing data protection regulations?
2) Do social and communication apps implement robust mechanisms to verify the age of their users?
3) After the enactment of the GDPR were there any changes in the age limits specified in the ToU and/or the mechanisms adopted by social and communication apps to verify the age of their users?

This study was commissioned by CyberSafeIreland, an Irish not-for-profit organization that aims to empower children, parents and teachers to navigate the online world in a safe and responsible manner. In our study we considered apps categorized in the social (Snapchat, Instagram, TikTok, HouseParty, Facebook) and communication (WhatsApp, Viber, Messenger, Skype, Discord) categories in the Google app store. According to the data collected from CyberSafeIreland's annual survey of children's use of social media [2], these are the most used social and messaging apps by children, aged 8-13. This study focused on mobile apps to reflect the usage of children in this age category: according to CyberSafeIreland [2], 92% of children own a mobile device, only 20% own a laptop and less than 10% own a desktop computer.

The set of the most popular apps has not changed between 2019 and 2020. **Table 1** shows a summary of our results for Snapchat, WhatsApp, Instagram, TikTok, and Viber. **Table 2** shows a summary of our results for Messenger, Skype, HouseParty, Discord, and Facebook. For each application we answered eight questions. Questions 1-2 address RQ1, while Questions 3-8 address RQ2. We indicate explicitly in both tables when the answer to a question has changed between 2019 and 2020. To answer RQ3 we compared the results obtained in the study performed in 2019 with those obtained in 2020.

We performed the study for the first time in April 2019 and repeated it in April 2020. Each study was conducted by one of the authors and the results were cross-validated by a different author. We acquired the ToU from the settings of each app and also online from the respective websites of each app. We installed each app on a new Nokia 2.3 smartphone, and attempted to create an account for three fake users aged 12, 13 and 16. To test each app we performed the sign-up by providing a date of birth —when requested— that suggested ages 12, 13, and 16. The interested reader can find the detailed results obtained for the top 10 apps in 2019 [6] and 2020 [7] online.

Terms of Use. 7 apps set the minimum age for using their service to 13 years in their ToU. WhatsApp set the age limit to 16 to take into account GDPR requirements. Although in 2019 Skype set the minimum age to 13, it removed this age limit in 2020. Thus, a user aged 12 or below can still create an account with parental consent. Discord does not state clearly the minimum age in its ToU. None of the apps takes into account the differences between the EU members w.r.t. the digital age of consent, except Facebook, Instagram, and Messenger that specify that in Spain the age limit is 14.

Request to provide an age during sign-up. WhatsApp and Discord are the only apps that do not require a user to input his/her age during sign-up.

Account creation for underage users. Among the apps that require users to provide an age during sign-up, 7 do not allow the creation of an account, when an age below the limit (12) is provided. Since 2020, only Skype allows the user to create an account after receiving parental consent via email.

Age verification. The app that, in our opinion, employs the most robust age verification mecha-

Table 1. Management of Underage Users in Snapchat, WhatsApp, Instagram, TikTok, and Viber.

Question	Snapchat	WhatsApp	Instagram	TikTok	Viber
1) What is the minimum age stated in the terms of use?	13	16	13	13	13
2) Is the minimum age the same across all EU countries?	Yes	16	No, in Spain is 14	Yes	Yes
3) Is it mandatory to input the age on sign-up?	Yes	No	Yes	Yes	Yes
4) If the answer to the previous question is yes, what happens if age 12 is entered?	Cannot create an account	N/A	Cannot create an account	Cannot create an account	Cannot enter age below 13
5) If you enter age 13, are there any additional verification processes?	No	N/A	Recommends to send an email to a parent	No	No
6) Is it possible to bypass the existing age verification process?	Yes, providing a false age	N/A	Yes, providing a false age	• Yes, providing a false age (2019) • No (2020)	Yes, providing a false age
7) If age 16 is entered on sign-up, is there any age verification process enabled?	No	N/A	No	No	No
8) At any point, is the minimum age made clear to the user?	Yes	Yes	Yes	Yes	Yes

Table 2. Management of Underage Users in Messenger, Skype, HouseParty, Discord, and Facebook.

Question	Messenger	Skype	HouseParty	Discord	Facebook
1) What is the minimum age stated in the Terms of Use?	13	• 13 (2019) • None (2020)	13	Unclear	13
2) Is the minimum age the same across all EU countries?	• Yes (2019) • No, in Spain is 14 (2020)	Yes	Yes	Yes	No, in Spain is 14
3) Is it mandatory to input the age on sign-up?	• No (2019) • Yes (2020)	Yes	Yes	No	Yes
4) If the answer to the previous question is yes, what happens if age 12 is entered?	• N/A (2019) • Cannot create an account (2020)	• Cannot create an account (2019) • Require parental consent via email (2020)	• N/A (2019) • Cannot create an account (2020)	N/A	• N/A (2019) • Cannot create an account (2020)
5) If you enter age 13, are there any additional verification processes (e.g. emailing a parent)?	No	Send an email to a parent	No	N/A	Optionally ask for parent approval
6) Is it possible to bypass the existing age verification process?	Yes, providing a false age	Yes, providing a false age	Yes, providing a false age	N/A	Yes, providing a false age
7) If age 16 is entered on sign-up, is there any age verification process enabled?	No	No	No	N/A	No
8) At any point, is the minimum age made clear to the user?	• No, in 2019 • Yes, in 2020	No	Yes	No	Yes

nism is the 2020 version of TikTok. During sign-up, it asks the user to enter his/her date of birth. If the user enters an age below 13 (e.g., 12), s/he gets a message stating that s/he is not eligible to sign-up. To create a TikTok account, a user would have to either supply proof of an age that is over or equal 13 to TikTok support or else sign-up on another device. However, if the user enters an age equal or over 13 from the start, s/he will be able to sign-up simply lying about his/her age. A less robust age verification mechanism is offered by Facebook. If the user enters an age below 13 during sign-up, s/he is prevented from creating a Facebook account. However, if the user enters an age equal or over 13 s/he can create an account without providing any proof to demonstrate his/her age. For 7 of the apps, a child can circumvent all age verification mechanisms by entering a false age. Besides TikTok, Messenger also makes it somewhat difficult to create an account as an older user, after attempting to sign-up as a 12 year old. It was indeed necessary to clear the cache and remove both Facebook and Messenger apps, in order to restart the sign-up process. With HouseParty, it was necessary to re-install the app to bypass the age verification mechanisms enacted during sign-up.

For users aged 13-15, 7 apps do not implement any age verification mechanisms. Only Instagram recommends asking a parent for approval to use the app, Facebook optionally gives a child the chance to ask for parental approval, and Skype, instead, requires the approval by a parent up to the age of consent.

However, if the age 16 is provided as input, none of the apps require a proof of age.

Minimum age during sign-up. All the apps make the minimum age to use their services clear during sign-up and/or in the ToU, with the exceptions of Skype and Discord. For some of the apps, such as Snapchat, the ToU suggest differences that the functionality may be restricted for 13-16 years old, without specifying how. Other apps, such as Viber, make no differences between the privacy settings for a 13 year old, and those for a 16 year old or older.

Changes after the enactment of GDPR. Although the age verification mechanisms analyzed are still insufficient to protect underage users, we noted a number of new developments since 2019, when the tests were first conducted. There are now some restrictions in place that might act as a deterrent to underage users. On certain apps, it is quite challenging after giving an initial age of 12, and being rejected, to start the sign-up process again pretending to be 13 or older. TikTok put in place the most difficult age verification mechanism to bypass, as a direct result of financial penalties imposed for non-compliance with data protection legislation.

Messenger now asks for an age during sign-up. It does not explicitly request parental consent for 13-15 year olds to create an account, but provides an option to change the privacy settings and get parental consent. This suggests that there are extra data protection measures in place for 13 to 15 year olds by default. Finally, Skype now accepts a user at age of 12, in direct contrast to most of the other apps which have a minimum age of 13. The app does however insist on the user obtaining parental consent, and this must be done via a Microsoft account.

USING BIOMETRICS FOR AGE VERIFICATION

A possible solution to implement more robust age verification mechanisms is to use biometrics features, that are unique to the app user. Thus, we analyzed advantages and disadvantages of some of the existing age recognition techniques using biometrics features, shown in **Table 3**. Speech recognition [8] has been adopted for age-group identification for children aged 5-16. Using specific regions in the speech bandwidth that contain the most important information for classification, this approach can achieve an accuracy of 85.8% in the best scenario. However, speech may not be a reliable feature for age recognition for children aged 11-13, due to variations in the timing of the onset of puberty. Also using speech recognition for age verification purposes can be bypassed easily by playing voice recordings.

Fingerprint characteristics [9], such as the Ridge Thickness to Valley Thickness Ratio and the Ridge Count have also been used for age group recognition. This approach has high accuracy (82.14%) and it is hard to circumvent, because it is difficult to falsify fingerprint readings. However, it does not guarantee the anonymity of the user and requires a fingerprint reader.

Table 3. Advantages and Disadvantages of Biometric Factors for Age Recognition.

Biometric Factor	Pros	Cons
Speech	• High accuracy • No additional hardware required	• Easy to circumvent • Low reliability for children aged 11-13
Fingerprint	High Accuracy	• Requires fingerprint reader • Limited anonymity
Face traits	• High Accuracy • No additional hardware required	Easy to circumvent
Ear	No additional hardware required	Less accurate
Iris	Low Accuracy	• Requires Iris Reader • Low Anonymity

Using facial features represents a promising avenue for age recognition. For example, Levi and Hassner [10] describe the use of a deep convolutional neural network (CNN) for age classification, using only three convolutional layers and two fully connected layers with a small number of neurons. This approach uses facial features, such as the distance measurements between facial points and the skin elasticity, and it is very effective especially with low quality images. On the one hand, since these facial features are insufficient to identify a user, age recognition techniques based on these features can ensure user anonymity. However, on the other hand, these age recognition techniques can also be circumvented easily using a picture of an adult.

Ear features extracted from anthropometric landmarks of the ear (distance measurements and area calculations) have also been adopted for age classification [11]. However, ear features are not a very decisive characteristic in a person growth and there is an insufficient amount of training samples for each age group. Thus, this approach has lower accuracy compared to the techniques based on speech, fingerprint and face traits.

Iris images have also been used to distinguish users between different age groups using a combination of a small number of geometric features [12]. However, in order to have good accuracy, this technique requires the use of a near infrared camera which may not always be available on a mobile device. Other researchers [13] have trained a classifier using iris images captured with a mobile phone obtaining a lower accuracy in age group identification. Because iris features are used for person identification, they are quite intrusive and may not ensure anonymity. In summary, the classification techniques for age recognition that have the highest accuracy have the limitation of either requiring additional hardware (fingerprint, iris) or to be easy to circumvent (speech, face features).

RECOMMENDATIONS

Existing data protection regulations are ineffective without clarity in relation to how age verification mechanism should be enforced in the ToU and in the implementation of apps. In reality, the application of substantial financial penalties (e.g., the case of TikTok) was the main trigger for app providers to implement more effective age verification mechanisms. Based on our study and on our survey about biometrics-based age recognition techniques, we propose the following recommendations to app providers and developers.

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 is presented 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. Thus, users must be incentivised to be honest about their age, with minimal data being collected in this case. Giving a user an option to go back and change their date of birth in order to bypass any restrictions encourages them to lie about their 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 the most sensible solution and the hardest to circumvent.

Implement Robust Age Verification Mechanisms. Where a minimum age requirement is put 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. Thus, we recommend age verification as an ongoing process that does not terminate after sign-up. For example, age verification can analyze information generated from the use of an app (e.g., texts, content exchanged) [14] to assess whether a user lied about his/her age at the moment of sign-up. Alternatively, an adult can enter the age of his/her child in the OS setting of the phone (like Android settings). During sign-up, apps can then obtain the age of a user directly from the phone settings.

CONCLUSION

This paper has the main objective to raise awareness about management of underage users in apps. We recommend app providers to increase robustness of the age verification techniques implemented during sign-up and to clarify the minimum age of use and the treatment of personal data. Because our recommendations do not take into account the specific functionalities of an app, they could be generalized to other apps that require to implement age limits in their ToU and/or robust age verification mechanisms. We focused our study on the mobile version of the top 10 social and communication apps among underage users. These apps were downloaded from the Irish app store. Thus, our results concerning robustness of age verification mechanisms may not be generalizable to the PC version of the top 10 apps or to the versions of the apps available in another geographical location (e.g., North America, Asia).

In future work, we will assess robustness of the age verification mechanisms adopted in the PC version of the app considered in this study. We will also perform empirical studies to understand a) how to present information about the minimum age and the treatment of data to users below 18, and b) which age verification solutions are most likely to be bypassed by young users. Finally, we will focus our attention on the specific differences in privacy settings and data collected by social and communication apps where a user has signed up and declared themselves to be aged 13-15 (with or without obtaining parental consent).

ACKNOWLEDGMENT

This work was partially supported by Science Foundation Ireland grant 15/SIRG/3501, EU H2020 CyberSec4Europe project grant 830929, and the ERC Advanced Grant no. 291652 (ASAP).

REFERENCES

1. Ofcom. - Children and Parents: Media Use and Attitudes report 2019. [Online]. Available: https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf
2. CyberSafeIreland - Annual Report 2018 [Online]. Available: https://cybersafeireland.org/media/1300/csi_annual_report_2018_w.pdf
3. nidirect government service - Social networking sites, online gaming and keeping children safe online [Online]. Available: https://www.nidirect.gov.uk/articles/social-networking-sites-online-gaming-and-keeping-children-safe-online
4. J. Horkoff, J. Ersare, J. Kahler, T. D. Jörundsson and I. Hammouda, "Efficiency and Effectiveness of Requirements Elicitation Techniques for Children," *Proc. of the IEEE 26th International Requirements Engineering Conference*, pp. 194-204, 2018. (conference proceedings)
5. Advertising Standard Authority - ASA research shows children are registering on social media under false ages [Online]. Available: https://www.asa.org.uk/news/asa-research-shows-children-are-registering-on-social-media-under-false-ages.html
6. P. Zippo, and L. Pasquale, "2019 Technical Report: a Review of Age Verification Mechanism for 10 Social Media Apps" [Online]. Available: https://arrow.tudublin.ie/cserrep/66/
7. C. Curley, "2020 Technical Report: a Review of Age Ver-

ification Mechanism for 10 Social Media Apps" [Online]. Available: https://arrow.tudublin.ie/cserrep/65/

8. S. Safavi, M. Russell, and P. Jančovič, "Automatic Speaker, Age-group and Gender Identification from Childrens Speech," *Computer Speech & Language*, vol. 50, pp. 141–156, 2018. (journal)
9. A. S. Falohun, O. D. Fenwa, and F. A. Ajala, "A Fingerprint-based Age and Gender Detector System using Fingerprint Pattern Analysis," *International Journal of Computer Applications*, vol. 136, no. 4, 2016. (journal)
10. G. Levi, and T. Hassner, "Age and Gender Classification Using Convolutional Neural Networks," *Proc. of the IEEE Conf. on Computer Vision and Pattern Recognition*, pp. 34–42, 2015. (conference proceedings)
11. D. Yaman, F. I. Eyiokur, N. Sezgin, and H. K. Ekenel, "Age and Gender Classification from Ear Images." *Proc. of the Int. Workshop on Biometrics and Forensics* , pp. 1–7, 2018. (conference proceedings)
12. M. Erbilek, M. Fairhurst, and M. C. D. C. Abreu, "Age Prediction from Iris Biometrics." *Proc. of the 5th Int. Conf. on Imaging for Crime Detection and Prevention*, pp. 1–5, 2013. (conference proceedings)
13. A. Rattani, N. Reddy, and R. Derakhshani, "Convolutional Neural Network for Age Classification from Smartphone based Ocular Images." *Proc. of the Int. Joint Conf. on Biometrics*, pp. 756–761, 2017. (conference proceedings)
14. C. Peersman, W. Daelemans, and L. Van Vaerenbergh, "Predicting Age and Gender in Online Social Networks." *Proc. of the 3rd Int. Workshop on Search and Mining User-Generated Contents*, pp. 37–44. 2011. (conference proceedings)