






# The Digital Loophole: Evaluating the Effectiveness of Child Age Verification Methods on Social Media

Fatmaelzahraa Eltaher<sup>1</sup><sup>a</sup>, Rahul Krishna Gajula<sup>1</sup><sup>b</sup>, Luis Miralles-Pechuán<sup>1</sup><sup>c</sup>,  
Christina Thorpe<sup>2</sup><sup>d</sup> and Susan Mckeever<sup>1</sup><sup>e</sup>

<sup>1</sup>*School of Computer Science Technological University Dublin, Ireland*

<sup>2</sup>*School of Informatics and Cybersecurity Technological University Dublin, Ireland*

{fatmaelzahraa.eltaher, rahul.gajula, luis.miralles, christina.thorpe, susan.mckeever}@tudublin.ie

**Keywords:** Age Verification, Age Assurance, Social Media, Child Safety, CSAM.

**Abstract:** Social media platforms are an integral part of daily life for nearly five billion people worldwide. However, the growing presence of underage users on these platforms raises significant concerns regarding children's exposure to harmful content and its impact on their mental health. This paper examines the effectiveness of age verification measures implemented on leading platforms Facebook, YouTube, Instagram, TikTok, Snapchat, and X. We evaluate the age verification processes required for account creation by simulating the registration steps for minors on these platforms. We also compare these methods to best practices in online age assurance in finance, betting and public transportation sectors. IEEE provides a standard for evaluating the age assurance of a platform or service. Our study benchmarks each platform's approach against the IEEE standard for robustness. Our research identifies gaps that allow underage users to easily bypass existing age restrictions, with particular practices such as allowing disposable emails and basic browser refreshes further weakening self-declared age checks. The findings highlight the need for more robust age verification measures by social media applications to support their stated age limit policies. This work emphasises the urgent need for stronger and more reliable age verification methods to align the digital age of consent across EU member states and beyond with the minimum age requirements on social media.

## 1 INTRODUCTION


Social media platforms (SMP) have become an essential part of modern life, with over five billion users globally in 2024, projected to exceed six billion by 2028 (Dixon, 2024). A few platforms dominate this space, including Facebook, YouTube, Instagram, TikTok, and Snapchat, attracting millions of users each month and making SMP one of the most widespread digital experiences worldwide (Statista, 2024).


While most platforms set a minimum age of 13, many younger children bypass these age restrictions. Children often falsify their ages—or receive help in doing so—to gain access, indicating that current age verification practices are insufficiently robust (Adib et al., 2023; Beresford et al., 2023; Childwise, 2023).


According to a Childwise survey conducted in the UK, 90% of children aged 11 to 12 already use SMP (Childwise, 2023). The survey also revealed that among children aged 8 to 12, 65% in England and 84% in Ireland have SMP or messaging accounts (de Souza, 2022; Beresford et al., 2023).


Social networks provide numerous opportunities for creativity, learning, and social engagement but also expose children to significant dangers. These risks can be categorised using the “4Cs of Online Risk” model, a widely recognised model for classifying children's key types of online risks. The model identifies four risk areas: Content (exposure to harmful material), Contact (interaction with dangerous individuals), Conduct (harmful behaviour as either victim or perpetrator), and Contract (commercial exploitation) (Livingstone and Stoilova, 2021).


In England, a survey of 2005 children and their parents found that 45% of children aged 8-17 encountered harmful content online (de Souza, 2022). In Indonesia, a survey revealed that nearly half (48.7%) of children aged 12-15 had been exposed to pornogra-

<sup>a</sup>  <https://orcid.org/0000-0002-9951-2019>

<sup>b</sup>  <https://orcid.org/0009-0004-0961-1892>

<sup>c</sup>  <https://orcid.org/0000-0002-7565-6894>

<sup>d</sup>  <https://orcid.org/0000-0002-2359-883X>

<sup>e</sup>  <https://orcid.org/0000-0003-1766-2441>

phy, with SMP being the entry point for 42.2%. Between March 28 and April 1, 2024, Snapchat conducted a survey of 1,037 US teens and young adults about their exposure to and awareness of online sexual crimes against minors. Key findings indicate that sexual-related online risks are widespread, with 68% of respondents reporting having shared intimate imagery or experienced grooming or catfishing behaviours (Beauchere, 2024). Across 25 European countries, 20% of children aged 9-16 reported viewing sexual content, and 8% said they had experienced cyberbullying (Staksrud et al., 2013).

The connection between SMP usage and mental health issues in children is becoming increasingly evident. Research indicates that SMP usage is associated with rising levels of anxiety, depression, and psychological distress among young users (Keles et al., 2020). In the UK, 70% of individuals aged 12 to 21 report experiencing anxiety, stress, or depression due to SMP use, yet only 7% say it stops them from using these platforms (Stem4, 2023). These findings highlight the need for stronger measures to prevent children, especially those under 13, from accessing these platforms. For older minors, access should be accompanied by supervision or stronger safeguards.

This paper examines the effectiveness of current age assurance mechanisms on SMP, contributing in several key areas:

1. **Assessment of Current Methods:** The paper tests the existing age verification processes for account creation on six leading platforms, identifying how processes can be bypassed.
2. **Highlighting Regulatory Gaps:** It explores the inconsistency between the digital age of consent across EU Member States and the minimum requirements enforced by SMP.
3. **Platform Rankings:** The paper ranks SMP based on compliance with IEEE standards for age assurance, including a comparative ranking of the platforms against each other.

The remainder of this paper is structured as follows: Section 2 explores legal frameworks for digital age consent and evaluates SMP's terms of service and age assurance methods. Section 3 describes the study's scope, experimental setup, and platform selection. Section 4 analyses the effectiveness of current age verification practices used by major platforms. Finally, Section 6 summarises the key findings.

## 2 LITERATURE REVIEW

This section explores the legal frameworks governing the digital age of consent and evaluates the terms of service implemented by SMP. Additionally, it analyses the various age assurance techniques applied across internet platforms, framing the challenges posed by SMP within a broader context.

### 2.1 Online Safety Regulations

The General Data Protection Regulation (GDPR) aims to harmonise data privacy laws across EU member states (GDPR, 2016). A key provision of the GDPR is the "age of digital consent", which mandates specific regulations for collecting and processing personal data from minors when consent is lawful. If a child is below the legal age of consent, online services must secure parental or guardian consent before processing any personal data (GDPR, 2016; EDPB, 2024).

Article 8 of the GDPR outlines the rules for collecting data from minors, generally requiring parental consent for children under 16 who are directly offered online services. However, EU member states can lower this age threshold if it does not exceed 13 (GDPR, 2016; Schofield, 2024; Milkaite and Lievens, 2019). Table 1 presents the digital age of consent in different EU countries.

Table 1: Digital Age of Consent in EU Member States.

Country	Digital Age of Consent
Belgium, Estonia, Finland, Latvia, Malta, Portugal, Sweden, Denmark, United Kingdom	13
Austria, Bulgaria, Cyprus, Italy, Lithuania, Spain	14
Czech Republic, France, Greece, Slovenia	15
Croatia, Germany, Hungary, Ireland, Luxembourg, Netherlands, Romania, Poland, Slovakia	16

Despite established regulations, SMP can still collect personal data from minors without parental consent under specific legal bases outlined in Article 6 of the GDPR (Data Protection Commission, 2023). Legal justifications include contractual obligations, official functions, or legitimate interests, emphasising that consent is only one of several bases for data processing (GDPR, 2016). Such flexibility raises concerns about potential loopholes: while parental consent is required in many instances, SMP may rely on alternative legal grounds to justify data collection, particularly if the service considers the processing necessary to fulfil user agreements (e.g., account creation).

In the United States, the Children's Online Privacy Protection Act (COPPA) is a US law that protects the privacy of children under 13 by regulating

how online services collect and handle their information. COPPA imposes similar requirements, mandating that websites and online services obtain parental consent before collecting user data under 13 (GDPR, 1998). The main SMP, except Tiktok, are based in the US. They make operational choices to ensure compliance with COPPA, and these choices affect children everywhere. If platforms are aware that there are users under the age of 13, they are subject to COPPA's regulations (GCHQ and DCMS, 2020).

The EU Digital Services Act (DSA) introduces stricter requirements for age verification to protect minors from accessing harmful content on digital platforms (Act, 2022). Regulators worldwide, including Arcom in France, An Coimisiún in Ireland, the KCSC in South Korea, and Ofcom in the United Kingdom, require regulated entities to implement age assurance systems as a compliance obligation (Network, 2024).

## 2.2 Social Media Terms of Use

SMP stipulate minimum age requirements in their terms of service, and this age may differ for a platform depending on the country. For instance, Facebook and Instagram require users to be 13 years old, but with exceptions in some countries such as South Korea, Spain, and parts of Canada (Quebec), where the minimum age is 14 (Meta, 2024a; Meta, 2024b). Similarly, platforms such as X (formerly Twitter) and Snapchat also require a minimum age of 13 (X, 2024b; Snapchat, 2024).

YouTube states that users aged 13 and over can create accounts, although parental consent is required for users under 18 (YouTube, 2024). As noted by TikTok, the minimum age requirement is 13 years old. For individuals under 13, TikTok provides a view-only experience in the US (TikTok, 2024b). Table 2 shows the age requirements stated by the main SMP.

Table 2: Age Requirements for Major Social Media Platforms.

Platform	Min Age	Region Min Age	Parental Consent
Facebook and Instagram	13	14 (*Exceptions in South Korea, Spain, and Quebec)	No
X	13	-	No
Snapchat	13	-	No
YouTube	13	-	Yes
TikTok	13	View-only for < 13 in US	No

Some countries set stricter age requirements for digital consent than those defined by SMP. This cre-

ates inconsistencies in countries such as Germany and Ireland, where the legal age for consent is 16, but SMP has stated lower age limits. Similarly, in Italy and Spain, children under 14 need parental permission to access online services. These apparent mismatches between national laws and platform policies undermine the effectiveness of national frameworks designed to protect minors in digital spaces.

## 2.3 Age Assurance Methods on Online Services and Platforms

Online services and platforms rely on various digital age assurance methods to verify that users meet the stated age limit. Age assurance involves three processes: age verification (using official identity documents), age estimation (employing technologies such as facial analysis), and self-declaration (where users provide their age) (Raiz Shaffique et al., 2024; Sas and Mühlberg, 2024).

Age assurance can be applied at the onboarding account creation and as a monitoring mechanism when the account is active. The critical point of age checking is at sign-up to pre-empt the onboarding of underage children onto platforms. This section reviews the age assurance methods described on the official websites of various online services and platforms. This involved identifying and analysing publicly available information on age assurance techniques, user requirements during account creation, and any age verification processes outlined by each platform. The various methods are detailed below. They are practical implementations of the three approaches to age assurance.

- 1. Self-Declaration:** It is the most commonly employed method for age assurance across online platforms such as Facebook, Instagram, TikTok, Snapchat, X, LinkedIn and YouTube (Diwanji, 2021; Franqueira et al., 2022; Google, 2024; Snapchat, 2024; X, 2021; LinkedIn, 2024). This approach requires users to input their age during account creation. This method has significant limitations as a robust method of age assurance, as minors can falsify their age. This method does not involve additional assurance steps, leading to widespread underage access to these platforms.
- 2. ID Verification:** In this age verification approach, users verify their age by uploading a verifiable ID, such as a birth certificate or passport. To enhance security, platforms may also require a selfie or photo of the user holding the ID to ensure authenticity. The storage of age-related information will depend on each service provider's specific use

cases.

SMP, including Facebook and Instagram, do not employ ID verification at account creation, using it only retrospectively if a platform user's age is under suspicion (Facebook, 2024a; Instagram, 2024a). Outside of social media, sectors with regulatory controls or revenue-based motivations use ID verification for their users to access services or products. Betting company PaddyPower uses ID verification if electronic checks to confirm eligibility for gambling are insufficient (PaddyPower, 2024). Financial services such as Revolut mandate ID verification and real-time selfies during account registration (Revolut, 2024). E-commerce platforms Amazon require both an ID and a selfie for purchasing age-restricted items (Amazon, 2024). Transport services that apply child discounts apply verification, such as the Irish Transport cards where a selfie and ID must be supplied (TFI, 2024). Similarly, Airbnb demands an ID photo, a selfie, and an ID photo based on the user's location or if anomalies are detected.

3. **Profiling:** This age estimation method relies on algorithms to estimate the actual age of users, but this is applied by SMP retrospectively when users have already created their accounts. For instance, Facebook and Instagram utilize various indicators, such as considering birthday wishes from others and the age mentioned in those messages (Diwanji, 2021). On the other hand, TikTok looks for terms or phrases in user-generated material that could indicate the creator is underage (TikTok, 2024a). Since these methods are not used during account creation, they do not prevent underage users from initially accessing the platforms.
4. **In-App Reports:** This age estimation method enables users to flag concerns about another user's age. After a report is made, the platform investigates age concerns. If X, Facebook, TikTok, or Instagram cannot confirm that the reported account is administered by an individual over 13, they will remove this reported account (X, 2024a; Facebook, 2024b; Instagram, 2024b; TikTok, 2024a). However, this mechanism applies only to active accounts and does not prevent underage users from accessing the platform initially. This delay poses significant risks, as it exposes minors to potential dangers until their age is verified.
5. **Third-Party Assurance:** Using this method, the user's age will be confirmed by another organisation. For example, if a user wants to update their age on Facebook or Instagram, they may be required to submit a video selfie to a third-party ser-

vice (age estimation)(Meta, 2024c; Meta, 2024d). Platform X uses third-party ID checks (age verification) to enhance trust for Premium users, ensure safety by preventing impersonation, and promote authenticity for creators in revenue-sharing programs. (X, 2024).

In summary, ID verification is used for account creation processes in regulated or revenue-motivated sectors. SMP rely on self-declaration for age assurance when users create accounts, with more robust methods such as ID verification applied only when underage use is suspected. The exact number of underage child accounts on SMP which are never flagged or suspected is still being determined. This highlights the urgent need for empirical studies to evaluate age assurance methods and measure how easily current age verification methods can be bypassed.

### 3 METHODOLOGY

This section outlines the scope, platform selection, and experimental setup employed in this study. Our study focuses on verifying the robustness of the age verification process at the critical account set-up stage, i.e. how effectively the current age verification protocols prevent underage users from accessing SMP.

#### 3.1 Criteria for Platform Selection

We identify the most widely used SMP globally based on social media usage statistics from Statista (Statista, 2024). This list is cross-referenced with a research study on child online safety and underage social media usage produced by Ofcom (Ofc, 2022).

Figure 1 shows the overall number of worldwide users of different SMP, and figure 2 shows the percentage of users within age groups on various SMP.

For this study, we focus on media-sharing SMP rather than messaging apps. As seen in figures 1 and 2, the most popular media-sharing platforms are YouTube, TikTok, Facebook, Instagram, Snapchat, and X.

#### 3.2 Methodological Approach to Age Verification Assessment

Our methodology consists of two steps. In the first step, we rank the platforms based on the effectiveness of their age assurance processes, using the IEEE framework as our benchmark for evaluation.

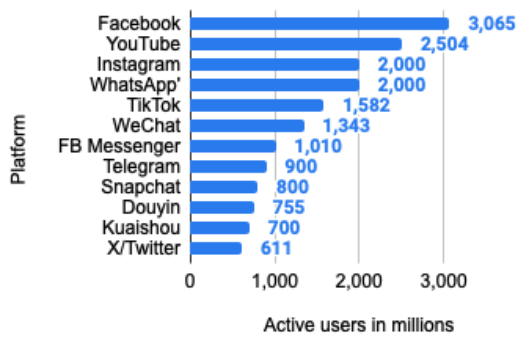


Figure 1: Most popular social networks worldwide as of April 2024, by number of monthly active users (in millions). Source: [Statista] (Statista, 2024).

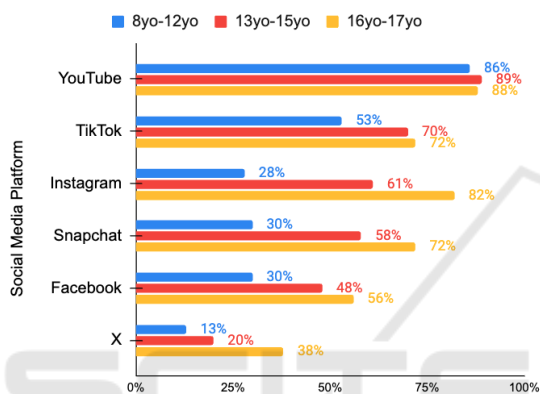


Figure 2: Percentage of minor users based on social media platforms based on age groups. [Source: OFcom (Ofc, 2022)].

In the second step, we attempt to create accounts below the designated minimum age limit and assess how easily the age verification mechanisms can be bypassed. We document whether additional checks, such as identity verification or parental consent, are triggered by each platform.

Additionally, we catalogue the types of verification used, which may include self-reported age, document uploads, or biometric checks, and evaluate whether these methods successfully prevent underage account creation.

## 4 EXPERIMENTS AND RESULTS

This section outlines the findings from testing the age assurance methods against each SMP.

### 4.1 Ranking the Level of Age Assurance

IEEE offers a standard for assessing a platform or service’s levels of age assurance (Society, 2024). This

standard establishes a framework for evaluating age assurance levels by defining confidence indicators across six key dimensions:

1. **Accuracy** – This measures how closely the verified or estimated age matches the user’s age.
2. **Frequency of Assurance** – How often the age check is repeated; Each use, weekly, monthly, annually Indefinite.
3. **Counter-Fraud Measures** – The extent to which the system prevents fraudulent attempts. At higher assurance levels, any contra-indicators (evidence of fraud) should be resolved or communicated to the relying party. These contra-indicators may remain unresolved in lower levels but must still be communicated.
4. **User Authenticity** – The ability to confirm the user is the same individual previously verified. The authentication levels range from Level 3, which includes liveness checks and advanced anti-spoofing measures (such as biometrics with a cryptographic key), to Level 0, which has no authentication or security measures. Levels 1 and 2 involve two-factor and single-factor authentication, respectively, with varying security and anti-spoofing technologies.
5. **Frequency of Authentication** – How often the user’s identity is confirmed.
6. **Birth Date Requirements** – Whether and how the specific birthdate is used.

The IEEE standard defines five normative combinations known as age assurance levels, ranging from minimal verification (Asserted) to the highest (Strict) level. These levels are established based on five key indicators, excluding the birthdate requirements indicator. The standard recommends considering these five levels before making specific adjustments to the required assurance level across one or more dimensions. These levels guide policymakers, regulators, and service providers in selecting appropriate age assurance measures for different contexts. The five levels are as follows:

1. **Asserted Age Assurance:** The Asserted level provides the least stringent age verification form. In this case, the user’s age is assumed based on self-declaration, with no checks in place to verify the accuracy of the asserted age. There are no fraud prevention measures or formal authentication of the user’s identity. This level typically involves indefinite verification, meaning the age is checked only once during registration and is not revisited later. This minimal level of assurance is suitable for services with no or very low risks to minors,

such as signing up for general newsletters aimed at children.

2. **Basic Age Assurance:** The Basic level provides minimal age assurance, involving low accuracy checks. The verification is typically conducted once and remains valid indefinitely unless revisited. Counter-fraud measures are communicated but minimal, with no user authentication implemented. This level is appropriate for accessing content intended for older children but not significantly harmful.
3. **Standard Age Assurance:** A moderate degree of accuracy is required at the Standard level, and checks are conducted annually. Counter-fraud measures are communicated but minimal, and user authenticity is verified at a higher level (Level 1). Monthly checks ensure that users remain eligible for the service, making this level appropriate for services with moderate risk, such as access to adult content.
4. **Enhanced Age Assurance:** The Enhanced level provides a higher verification level with monthly checks. Accuracy is enhanced, and counter-fraud measures are more stringent, requiring the resolution of any fraud indicators before proceeding. User identity is authenticated every time at Level 2. This level is suitable for services that involve higher risk, such as online gambling.
5. **Strict Age Assurance:** The Strict level represents the highest standard of age assurance, with frequent (weekly) checks, accuracy, and strict counter-fraud measures. Authenticity is verified at Level 3 at each use, ensuring the user’s identity is rigorously authenticated. This level is reserved for high-risk services, such as purchasing offensive weapons.

These five levels of age assurance provide a scalable framework for verifying age based on the risks associated with specific services or content. Lower levels of assurance (Asserted or Basic) may be sufficient for services with minimal risks. However, services that pose significant risks, such as gambling, accessing adult content, or purchasing dangerous items, require higher levels of assurance (Enhanced or Strict).

According to the IEEE standard, services relying on self-declaration for age verification are classified at the “Asserted level”. As illustrated in Figure 3, the age assurance methods employed during account creation by six major SMPs—Facebook, YouTube, Instagram, TikTok, Snapchat, and X—fall under this category. Our evaluation also extended to various online services, including Revolut, Paddypower, Airbnb, and

Transport Cards. Our analysis revealed gaps in the intermediate levels of age assurance (“Basic”, “Standard”, and “Enhanced”). We did not identify any applications that employ these levels during account creation.

Strict	5	Revolut, Paddypower, Airbnb, Transport Cards
Enhanced	4	
Standard	3	
Basic	2	
Asserted	1	Snapchat, Facebook, Instagram, YouTube, X, TikTok
None	0	

Figure 3: Ranking of age assurance methods across different applications according to IEEE standard.

While SMP generally implements an “Asserted” level of age assurance, these other services enforce a “Strict” level. SMP reliance on weak verification methods. This underscores the necessity of safeguards to protect minors effectively.

## 4.2 Account Creation Process

To extensively examine the age assurance methods utilized by SMPs and explore potential improvements, we designed a series of checks and applied them to six selected platforms: TikTok, X, Facebook, Instagram, YouTube, and Snapchat. The experiment was conducted on a desktop using Google Chrome in Dublin, Ireland, between 04/11/2024 and 08/11/2024. The experiments were conducted by three academic researchers.

We tested the robustness of age verification mechanisms by simulating account creation using different age inputs. Initially, we set the user’s date of birth to 1/1/2012 (indicating an age of 12) with a disposable email to evaluate whether platforms blocked users under 13. Next, we refreshed and changed the date of birth to 1/1/2011 (indicating an age of 13) while still using a disposable email address to observe if platforms blocked the disposable email or imposed additional security checks while using a disposable email address. Finally, we repeated the test with the same 01/01/2011 date of birth but switched to a valid email

to determine if platforms block users after multiple failed attempts. This process was done twice per platform to ensure repeatability and reliability.

1. **Is Age Verification Mandatory Through a Valid ID and Liveness Check?:** Compliance with this check would prevent users under 13 from falsifying their age. Each platform is tested to check if users must upload a valid government ID, such as a birth certificate, to verify their age during account creation. ID verification links the user to an official document with their date of birth and photo, making it difficult for children to bypass age restrictions. This is often combined with a “liveness check”, where users take a selfie to match the ID. These verification measures are necessary for underage users to easily create accounts, exposing a significant gap in preventing children from accessing age-restricted platforms.
2. **Are Disposable Emails Blocked?:** Disposable emails are temporary email addresses that users can create for short-term use, often to avoid spam or protect their privacy, which expires after a set period or can be discarded after use. This test checks if platforms block disposable emails like TempMail and YOPmail, as allowing them undermines security and age verification by enabling users to create multiple anonymous accounts.
3. **Is the Browser Session Refresh Exploits Prevented?:** This test examines whether refreshing the browser during signup allows users to bypass age checks. If refreshing enables users to re-enter birthdates, they can repeatedly try invalid ages until one meets the platform’s requirements, creating a loophole that allows underage users to bypass verification.
4. **Is an Image/Selfie Upload Required During Signup?:** This test checks if platforms require a selfie or photo upload during account creation to confirm user authenticity. Requiring a photo helps deter underage users by adding a visual layer to age verification.
5. **Is Changing the Age after Signup Prevented?:** This test investigates whether users can alter their age after creating an account. Changing the age post-signup can grant access to age-restricted content or features, such as mature content, which poses a risk if underage users can change their birthdate easily.
6. **Has Age Verification Improved Since 2020?:** This test assesses whether platforms have updated their age verification methods since (Pasquale and Zippo, 2020) in 2020. Regular updates to verification processes are essential to adapt to new threats

and ensure that platforms effectively prevent underage account creation. For instance, Facebook now requires a selfie upload at signup. X has prevented users under 13 from changing their age by disabling accounts created with an underage birthdate and blocking associated emails.

7. **Are Default Privacy Settings Applied to Users Under 18?:** This test assesses whether platforms provide a default privacy setting for users who have defined their age as under 18. Private profiles reduce exposure to unknown followers and content.
8. **Is there a Screen Time Limit for Users Whose (Self-Declared) Age is Under 18:** This test checks if platforms enforce a default screen time limit for users under 18. Limiting screen time helps protect younger users from excessive usage and exposure to potentially harmful content such as violence, eating disorder promotions, cyberbullying, and possibly online sexual abuse, especially without parental supervision.
9. **Are Parents Notified When Users Under 18 Sign Up?:** This step checks if parents are notified when their child creates an account, especially for children under 18 (allowing that this will only be triggered if their child has supplied an under-18 date of birth). Parent notification adds an extra layer of oversight, allowing parents to monitor their child’s online activity and ensure compliance with age restrictions.

Table 3 presents the results of the account creation processes across six social media platforms, as well as Transport Cards (such as Irish Leap cards, Oyster Cards in the UK, and Touch ‘n Go cards in Malaysia), Paddypower (an online gambling platform), Revolut (an online banking service), and Airbnb. This comparison highlights the effectiveness of age assurance and verification protocols across different platforms.

The rows with test steps highlighted in blue represent the age verification steps and check the account creator faces at the signup phase. In contrast, the rows with test steps highlighted in orange represent the age checks and features the platforms provide after the user has created an account.

Accounts were created solely for the research purpose of verifying account set-up details. No connections or interactions were made with other users. Once the experiments finished, the accounts were deleted.

Table 3: Age verification test results across SMP and sample other online services. Q1 - “During registration” is the most relevant as it guarantees truthful verification.

Test Step	Social Media Platforms						Other Online Services			
	Instagram	Facebook	X	Snapchat	TikTok	YouTube	Travel Card	Paddy Power	Revolut	Airbnb
1.- Is age verification mandatory through a valid ID/Passport, and are users under 13 prevented from falsifying their age?	X	X	X	X	X	X	✓	✓	✓	✓
2.- Is an image/selfie upload required during signup?	X	✓	X	X	X	X	✓	✓	✓	✓
3.- Are disposable emails blocked?	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
4.- Is the browser session refresh exploit prevented?	X	X	✓	X	X	X	✓	✓	✓	✓
1.- Is changing the age after signup prevented?	✓★	✓★	✓	✓	✓	X	N/A	N/A	N/A	N/A
2.- Has age verification improved since 2020?	✓	✓	✓	✓	✓	✓	N/A	N/A	N/A	N/A
3.- Are default privacy settings applied to users under 18?	X	X	X	X	✓	X	N/A	N/A	N/A	N/A
4.- Is there a screen time limit for users under 18?	X	X	X	X	✓	X	N/A	N/A	N/A	N/A
5.- Are parents notified when users under 18 sign up?	X	X	X	X	X	✓	N/A	N/A	N/A	N/A
	During registration phase						After registration phase			

★ A valid ID is required for age change after account signup.

## 5 DISCUSSION

The previous literature underscores shortcomings in social media platforms (SMPs) age assurance systems (Pasquale et al., 2020; Pasquale and Zippo, 2020), highlighting the need for further research to assess whether more robust solutions have been effectively implemented. This study reaffirms that the current age assurance mechanisms used by major SMPs allow users to bypass age restrictions by providing false information. This exposes minors to risks such as harmful content and mental health problems. In contrast, sectors like government transport cards (e.g., Irish Transport Cards), financial institutions (e.g., Revolut), online gambling platforms (e.g., PaddyPower), and accommodation services (e.g., Airbnb) use stricter age verification systems. These include government-issued ID checks and biometric verification, offering greater accuracy and security.

Facebook’s recent update to include selfie verification during account setup represents a step forward in age assurance compared to other platforms. The Facebook selfie verification system demonstrates mixed effectiveness. Some accounts created with valid emails and an appropriate age (13 years) were approved without selfie requests. Although the system successfully disabled accounts using an AI-generated image or an underage DOB, its inconsistency in requesting selfies highlights potential gaps in enforcing age restrictions uniformly. Until ID-based date of birth verification is implemented, the system

remains vulnerable to circumvention, such as using someone else’s photo to bypass selfie verification.

According to the IEEE standard, age assurance on YouTube, TikTok, Instagram, Snapchat, and X is inadequate (asserted). Although these platforms implement age-screening procedures to comply with the Children’s COPPA, they rely on self-declaration, pushing the burden of age verification on minors. This situation highlights the pressing need for legislation that mandates more effective age assurance methods from SMP.

Robust age-assurance techniques are crucial for preventing underage users from accessing SMPs. These techniques should be integrated into account creation to protect children from harmful content. SMPs could adopt models similar to platforms such as PaddyPower, Airbnb, and Revolut, where government-backed ID and biometric checks enhance age verification systems. Additionally, two-factor authentication (2FA) tailored for age assurance could be introduced. 2FA requires users to provide two distinct forms of identification (e.g., password and phone validation). This could include physical identity tokens or hardware-based authentication, ensuring that younger users cannot easily bypass age restrictions.

## 6 CONCLUSION

SMP has become part of everyday life for most people, particularly for younger users. However, de-



spite the age restrictions implemented by various platforms, underage users frequently circumvent these measures, exposing themselves to harmful content and increasing the risks of mental health problems.

This paper evaluates the current age assurance methods employed by popular platforms, including Facebook, YouTube, Instagram, TikTok, Snapchat, and X. By simulating account creation for minors, we confirm the reliance on self-declared age assurance rather than robust ID-based age verification and note the platform-specific gaps such as disposable email use and browser refreshes for validation skipping. We contrast these methods with the more robust verification approach the other sectors utilise, such as online betting and public transportation, which incorporates multi-factor checks, such as government-issued IDs and biometric verification. Additionally, we apply the IEEE standard to assess the effectiveness of platforms in safeguarding children.

This paper highlights the weakness of age assurance in SMP at the account creation stage. It underscores the urgent need for more robust solutions that extend beyond self-declaration. We recommend enhancements to current techniques, including AI-driven age assurance and government verification processes. The most viable solution is for governments to mandate that SMP implement stricter age verification methods.

For future work, it is worth exploring the alignment between the service and assurance levels outlined in the NIST SP 800-63 guidelines and the social networks.<sup>1</sup>

## ACKNOWLEDGEMENTS

This paper is part of the N-Light project funded by the Safe Online Initiative of End Violence and the Tech Coalition through the Tech Coalition Safe Online Research Fund (Grant number: 21-EVAC-0008-Technological University Dublin).

## REFERENCES

- (2022). Ofcom, children and parents: media use and attitudes report (2022). <https://www.ofcom.org.uk/media-use-and-attitudes/media-habits-children/children-and-parents-media-use-and-attitudes-report-2022>(archived on 2024-8-22).
- Act, D. S. (2022). Digital services act.
- <sup>1</sup>NIST SP 800-63 is Digital Identity Guidelines, For more information, visit <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>
- Adib, A., Zhu, W.-P., and Ahmad, M. O. (2023). Improving age verification technologies in canada: Technical, regulatory and social dynamics. In *2023 IEEE International Humanitarian Technology Conference (IHTC)*, pages 1–6. IEEE.
- Amazon (2024). Id verification amazon. Archived on 2024-08-29.
- Beauchere, J. (2024). A first-of-its-kind campaign to combat online child sexual exploitation and abuse.
- Beresford, O., Cooney, A., Keogh, A., Flynn, E., and Messena, M. (2023). Keeping kids safer online. online safety matters. trends and usage report academic year 2022/2023.
- Childwise (2023). Underage social platform usage: Research with children aged 11-14.
- Data Protection Commission (2023). Children’s data and parental consent.
- de Souza, D. R. (2022). Digital childhoods: a survey of children and parents.
- Diwanji, P. (July 27, 2021). Meta age verification methods. <https://about.fb.com/news/2021/07/age-verification/>(archived on 2024-8-29).
- Dixon, S. J. (May 17, 2024). Number of social media users worldwide from 2017 to 2028. <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/>.
- EDPB (2024). Process personal data lawfully. Archived on 2024-8-29.
- Facebook (2024a). Confirming age in facebook. [https://www.facebook.com/help/159096464162185?helpref=faq\\_content](https://www.facebook.com/help/159096464162185?helpref=faq_content)(archived on 2024-8-29).
- Facebook (2024b). Report a child account in facebook. [https://www.facebook.com/help/157793540954833/?helpref=related\\_articles](https://www.facebook.com/help/157793540954833/?helpref=related_articles)(archived on 2024-8-29).
- Franqueira, V. N., Annor, J. A., and Kafali, O. (2022). Age appropriate design: Assessment of tiktok, twitch, and youtube kids. *arXiv preprint arXiv:2208.02638*.
- GCHQ and DCMS (2020). Verification of children online (voco) phase 2 report. Multi-stakeholder Research Project.
- GDPR (1998). Children’s online privacy protection rule. Archived on 2024-8-29.
- GDPR (2016). General data protection regulation. Archived on 2024-8-29.
- Google (2024). Account on youtube. Archived on 2024-08-29.
- Instagram (2024a). Confirming age in instagram. [https://help.instagram.com/271237319690904/?helpref=related\\_articles](https://help.instagram.com/271237319690904/?helpref=related_articles)(archived on 2024-8-29).
- Instagram (2024b). Report a child account in instagram. <https://help.instagram.com/517920941588885>(archived on 2024-8-29).
- Keles, B., McCrae, N., and Grealish, A. (2020). A systematic review: The influence of social media on depression, anxiety and psychological distress in adolescents. *International Journal of Adolescence and Youth*, 25:79–93.
- LinkedIn (2024). Account on linkedin. Archived on 2024-08-29.

- Livingstone, S. and Stoilova, M. (2021). The 4cs: Classifying online risk to children.
- Meta (2024a). Facebook minimum age requirement. Archived on 2024-8-22.
- Meta (2024b). Instagram minimum age requirement. Archived on 2024-8-22.
- Meta (2024c). selfie age verification in facebook. Archived on 2024-08-29.
- Meta (2024d). selfie age verification in instagram. Archived on 2024-08-29.
- Milkaite, I. and Lievens, E. (2019). The changing patchwork of the child's age of consent for data processing across the eu. *Better Internet for Kids*.
- Network, G. O. S. R. (2024). Regulatory index.
- PaddyPower (2024). PaddyPower. Archived on 2024-08-29.
- Pasquale, L. and Zippo, P. (2020). A review of age verification mechanism for 10 social media apps.
- Pasquale, L., Zippo, P., Curley, C., O'Neill, B., and Mongiello, M. (2020). Digital age of consent and age verification: Can they protect children? *IEEE software*, 39(3):50–57.
- Raiz Shaffique, M., van der Hof, S., et al. (2024). Mapping age assurance typologies and requirements: Research report.
- Revolut (2024). Id verification revolut. Archived on 2024-08-29.
- Sas, M. and Mühlberg, J. T. (2024). Trustworthy age assurance? In *The Greens Cluster: Social & Economy, Location: The European Parliament*.
- Schofield, M. (2024). Eu age consent. Archived on 2024-8-29.
- Snapchat (2024). Age limitation in snapchat. Archived on 2024-08-29.
- Society, I. C. T. (2024). Ieee standard for online age verification.
- Staksrud, E., Ólafsson, K., and Livingstone, S. (2013). Does the use of social networking sites increase children's risk of harm? *Computers in human behavior*, 29(1):40–50.
- Statista (2024). Most popular social networks worldwide as of april 2024, by number of monthly active users. <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>.
- Stem4 (2023). Anxious and at breaking point. July 2023 Survey.
- TFI (2024). Leap card. Archived on 2024-08-29.
- TikTok (2024a). Removing suspected underage accounts from tiktok. Archived on 2024-08-29.
- TikTok (2024b). Tiktok minimum age requirement. Archived on 2024-8-22.
- X (2021). X age verification methods. <https://help.x.com/en/using-x/parental-consent>(archived on 2024-8-29).
- X (2024). Confirming age in x. <https://help.x.com/en/rules-and-policies/verification-policy>(archived on 2024-8-29).
- X (2024a). Report a child account in x. <https://help.x.com/en/forms/safety-and-sensitive-content/underage-user/x>(archived on 2024-8-29).
- X (2024b). X minimum age requirement. Archived on 2024-8-22.
- YouTube (2024). Youtube minimum age requirement. Archived on 2024-8-22.