TRUSTWORTHY AGE ASSURANCE?

A risk-based evaluation of available and upcoming age assurance technologies from a fundamental rights perspective.

Martin Sas
KU Leuven, Centre for IT & IP Law,
Leuven, Belgium

Jan Tobias Mühlberg
Université Libre de Bruxelles, Ecole Polytechnique,
Brussels, Belgium

February 2024

THE GREENS/EFA in the European Parliament

TABLE OF CONTENTS

ACKNOWLEDGMENTS

This report has been commissioned by the Greens/EFA Group at the European parliament. The authors conducted their research and analysis with complete independence, adhering to the highest standards of scientific integrity. The authors explicitly disclaim any responsibility for the political use of the study's findings.

The authors extend their appreciation to the interviewees who generously shared enlightening insights from their unique perspectives. All quotes included in this report have been confirmed for publication by each interviewee. However, it's important to note that these confirmations do not imply approval or endorsement of any arguments or conclusions presented in this report.

EXECUTIVE SUMMARY

Children represent a substantial portion of internet users, which creates an imperative to create a safe and secure online environment. Harmful content, however, is easily accessible, with 19% of respondents to a recent survey admitting exposure to pornography before the age of 13,[1] 14% reporting being threatened, and 45% reporting verbal abuse online.[2] Most providers of adult-restricted online content rely on self-declaration of age without further validation, which has proven to be ineffective and easy to bypass. Consequently, governments are urging the implementation of robust online age assurance systems that prevent children from accessing adult-restricted content or other types of harmful content online. Legislation aimed at improving online child protection, e.g., GDPR, AVMSD, DSA and age-appropriate design codes, consider age assurance as a protective measure and support their implementation online.

Age assurance measures are, however, controversial and raise concerns about their impact on the fundamental rights of both adults and children, since all internet users would need to prove they are adults to access specific content. This requirement, besides being intrusive regarding individuals' privacy, can potentially restrict individual's ability to freely express themselves and engage with others unless they provide personal information and have the capacity to go through an age assurance process. This specifically affects already marginalised populations who, e.g., do not possess the means for electronic identification, or for whom, e.g., facial scanning proves technically or personally impractical. Thus, fundamental rights including privacy, data protection, non-discrimination, freedom of expression, and freedom of association, are at risk if age assurance measures are not implemented in a proportionate, inclusive, and privacy-preserving way.

Moreover, age assurance measures may hinder children's development by preventing them from accessing certain content or services, even though these resources could potentially help them enhance their skills and media literacy, especially in recognizing and handling specific risks (e.g., social media) or in navigating difficult personal situations. In this context, alternative measures of protection, such as safer algorithmic recommendation, harmful content warnings or panic buttons, may be better suited to support children in their exploration of the online world. Striking a fair balance between protection and empowerment is therefore crucial, and the best interest of the child should be considered when assessing the necessity of implementing age assurance. Such assessments must take the type of content or service, the context in which children may access it, the evolving capacities of children, and the privacy intrusion of the age assurance methods into account.

1 "Questions doubts and hopes. Young people's attitudes towards age assurance and age-based restriction of access to online pornography," Australian Government, 2023, [21].
2 "The 2022 National Online Safety Survey – summary report," Australian Government, 2022, [120]

This study highlights the potential risks and benefits stemming from the use of age assurance technologies in the online environment, in particular regarding their impact on individuals' fundamental rights and children's rights. We conducted interviews with researchers, civil society organisations, age assurance tools' providers and regulatory authorities to gather insights on the readiness of age assurance technologies, the associated risks and their impact on children protection online. We synthesise the interviewees' contribution in the form of quotations, highlighted throughout this study. Via desktop research, we reviewed the relevant legal framework and analysed literature on age assurance to identify associated risks and to assess whether these technologies could be in tension with the protection of fundamental rights. We evaluated a wide range of age assurance technologies by assessing the extent to which each technology could protect children from harmful content, as well as the potential negative impact on fundamental rights, including children's specific rights.

We conclude that, while there is a clear need for protecting children online, there are currently no age assurance method that adequately protect individuals' fundamental rights. The risks associated with the implementation of age assurance include privacy intrusion, data leak, behavioural surveillance, identity theft, and impeded autonomy. Moreover, while none of the methods reviewed could attest user's age with certainty, the implementation of such measures may exacerbate existing discrimination against already disadvantaged groups of society, likely widen the digital divide and lead to further exclusion.

Promising privacy-preserving techniques, e.g, digital identities and double-blind transmission methods, are under development. These may offer improved user privacy protection by enabling anonymous age assurance. However, important security and inclusivity risks remain. Moreover, these technologies face implementation challenges, given the current absence of a pan-European technical and legal framework to support their wide adoption.

To guarantee individuals' fundamental rights online, there is an urgent need for mandatory risk assessments including fundamental rights, data protection and children's rights impact assessments. These must aim at striking a fair balance between children's protection and empowerment. Additionally, a comprehensive framework of standards, certification schemes, and independent audit controls must be established to ensure the safety and trustworthiness of age assurance measures and the accountability of technology providers.

In summary, our study reveals a misalignment between the urgency with which governments are pushing for age assurance and the time needed to develop robust, safe and trustworthy age assurance technology. The primary risk lies with the adoption of assurance solutions without adequate protection of individuals' fundamental rights, which could normalise excessive privacy intrusion and heightened risks of data leak and misuses across the online world.

LIST OF ABBREVIATIONS

- AI: Artificial Intelligence
- Arcom: Autorité de régulation de la communication audiovisuelle et numérique
- API: Application Programming Interface
- AVMSD: Audiovisual Media Services Directive
- AVPA: Age Verification Providers Association
- BfDI: Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- CFREU: Charter of the Fundamental Rights of the European Union
- CNIL: Commission National de l'informatique et des libertés
- CRIA: Children Rights Impact Assessment
- CSAR: Proposed Regulation laying down rules to prevent and combat child sexual abuse
- DLT: Distributed Ledger Technology
- DPA: Data Protection Authority
- DPC: Irish Data Protection Commission
- DPIA: Data Protection Impact Assessment
- DSA: Digital Services Act
- ECHR: European Convention of Human Rights
- EDPB: European Data Protection Board
- EDPS: European Data Protection Supervisor
- eID: Electronic Identification
- eIDAS: Electronic Identification Authentication and trust Services
- EU: European Union
- EUDI Wallet: European Decentralised Identities Wallet
- FRIA: Fundamental Rights Impact Assessment
- GDPR: General Data Protection Regulation
- ICO: Information Commissioner Office
- ID card: Identity card
- ISPs: Internet Service Providers

- ISS: Information society services
- JuSchG: Jugendschutzgesetz
- JMStV: Jugendmedienschutz-Staatsvertrag
- KJM: Kommission für Jugendmedienschutz
- LINC: Laboratoire d'Innovation Numérique de la
- MITM attack: Man-in-the-middle attack
- NFT: Non-fungible token
- NGO: Non-governmental organisations
- Ofcom: The Office of Communications
- PEReN: Pôle d'Expertise de la Régulation Numérique
- SREN proposal: Projet de loi visant à sécuriser et réguler l'espace numérique
- SSI: Self-Sovereign Identities
- UDHR: Universal Declaration of Human Rights
- UK: United Kingdom
- UN: United Nations
- UNCRC: United Nations Convention on the Rights of the Child
- US or USA: United States of America
- VPN: Virtual Private Network

INTRODUCTION

In our ever-connected modern society, internet is as omnipresent in children's lives as it is in adults'. Although, most online services are not age-appropriately designed and leave children exposed to various types of risks [69]. Acknowledging the pressing need to better protect minors online, regulators are increasingly turning towards age verification measures. Under European law, the Audiovisual Media Service Directive (AVMSD) [113] and the Digital Service Act (DSA) [116] both consider age verification as a protective measure, notably on social media and online video-sharing platforms (see Sections **2.2.** and **2.3.**). However, these acts only rely on age verification as an optional measure subject to necessity and proportionality assessments. Several age-appropriate codes also recommend the implementation of age verification without mandating it [18,54,56,78,97].

Nevertheless, in the light of the legislative initiatives currently emerging in various jurisdictions, regulators are now shifting towards mandatory age verification for an expanding range of online services, including some which are not inherently age-restricted (e.g., social media, instant messaging apps, and online video games). While pornography remain the primary focus of regulatory intervention - notably in France [65,67,68], in the United Kingdom [119], in the United States [85–87,92–94,96,98], in Canada [95], and more recently in Ireland [16bis] and Spain [83] - legislative acts mandating age verification on social media platform were adopted, both in France [66] and in the UK [119]. At the European level, the CSAR proposal [115] which aims to fight child sexual abuse online, proposes age verification as a mandatory mitigation measures, each time a software application could potentially be used for the purpose of children solicitation (i.e., grooming) (see Section **2.4.**). Finally, age verification measures are also taken into account by data protection authorities when assessing whether data controllers comply with their obligation under the General Data Protection Regulation (GDPR) [112], as the combination of articles 8 and 25 of the Regulation requires them to implement appropriate measures to protect children's data by design (see Section **2.1.**).

Meanwhile, the industry adapts rapidly. Major online services, such as Youtube [43], Yubo [133], Instagram [75], Roblox [90], Epic Games [29,30] or OnlyFans [131], are now implementing age verification measures beyond the mere declaration of age and involve, e.g., facial analysis or hard identifiers.

While age verification measures pursue a legitimate objective in protecting children against the adverse effects of certain online services, their implementation in a substantial part of the digital landscape raise important concerns. Building on previous research [1,24,31,40,84,126,127] and opinions from data protection authorities [19,20,55], as well as interviews with relevant stakeholders, this report evaluate currently available and upcoming age assurance methods in the light of the risks they may create for the

fundamental rights of individuals, both adults and children. Chapter **1** first clarifies the terminology used throughout the study, notably regarding the difference between age assurance and age verification. Chapter **2** then provides a thorough contextualisation of the regulatory framework applicable to age verification at the European level and emphasises the requirement for impact assessments to determine the necessity and proportionality of age assurance measures. Accordingly, Chapter **3** identifies potential risks stemming from the implementation of age assurance measures in online service. Chapter **4** evaluates the extent to which different age assurance technologies (see Section **4.1.**), as well as methods for transmitting the proof of age among multiple stakeholders (see Section **4.2.**) increase or mitigate the risks identified in Chapter **3**. A summary of the evaluation findings is available in Section **4.3.**), alongside a summary table (see **Table 4.13.**).

Our evaluation demonstrates that none of the currently available methods can cumulatively ensure a high degree of reliability in establishing someone's age while preventing circumvention and preserving privacy. The invasive collection of personal data necessary to ensure a high degree of age assurance exposes users, both adults and children, to heightened risk of behavioural profiling, data breach and potential misuse. Besides, both age estimation and age verification reveal themselves discriminatory towards a significant portion of the population, fostering social exclusion (see Sections **4.1.2.** and **4.1.1.**). Promising technologies currently under development can provide enhanced user privacy (see Sections **Age token**, **Digital Identity Wallets,** and **Double-Blind Method**). However, challenges remain notably regarding security, inclusivity and feasibility issues. To ensure that appropriate mitigation measures are implemented to minimise the risks identified and evaluated in Chapters **3** and **4**, regular independent auditing of age assurance solutions should be performed based on a comprehensive standardisation and certification framework. As outlined in Chapter **5**, several frameworks exist or are currently in development, both at international and national levels. However, to ensure the harmonisation across Member States and guarantee the highest levels of privacy, security, inclusivity and effectiveness in age assurance methods, we recommend the development of standardisation and certification frameworks at European level (see Section **5.2.**). Further recommendations are also provided to relevant stakeholders in the conclusion of the report (see Section **Recommendations**).

OBJECTIVES, METHODOLOGY, AND DEFINITIONS

Objectives

The purpose of this study is to evaluate the impact of available and upcoming age assurance technologies on fundamental rights, including children's specific rights.

Methodology

We conducted semi-structured interviews to gather insights on the readiness of age assurance technologies, the associated risks and their impact on children and society as a whole. Our questions covered issues such as the necessity for age assurance measures in online services; the impact of age assurance on users (especially children); the criteria for determining which age assurance method is appropriate for a specific service; the risks associated which certain methods and how user's personal data may be misused for other purposes than age assurance; the role of impact assessments, standards and certification schemes; the opportunities and challenges of digital identities and wallets as age assurance solutions (notably under the eIDAS 2 proposal) (see Section **Electronic Identification (eID) and Digital Identities** and Section **Digital Identity Wallets**); the opportunities and challenges related to the implementation of a double-blind approach (see Section **Double-Blind Method**)

]); and the existence of potential alternative measures to age assurance. We synthesised the interviewees' contribution in the form of quotations highlighted throughout this study.

The persons interviewed for this study encompasses 5 women and 6 men who respectively represent the research community, the civil society, the age assurance industry, or supervisory authorities. Among the 11 interviewees, 5 were based in the United Kingdom. This prevalence of interviewees residing in the United Kingdom is not intended by the authors but can be explained by the leading role that the UK have in the development of age assurance. One of the interviewees preferred to remain anonymous. The full list of the interviewees is available here:

- **Alexandra Zeeb-Schwanhäußer**: Representative of the German Federal Commissioner for Data Protection and Freedom of Information (Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)).
- **Duncan McCann**: Head of Policy Implementation at the 5Rights Foundation, an internationally active NGO which researches and advocates for a digital world where children can participate in the digital world creatively, knowledgeably and fearlessly.

- **Han Hye Jung**: Research and Advocate in the Children's Right Division of Human Rights Watch, an international NGO which investigates and reports on human rights abuses happening in all corners of the world.
- **Jen Persson**: Director of Defend Digital Me, a civil liberties group founded in 2015 to campaign for safe, fair, and transparent children's data in education.
- **Joris Duguépéroux, PhD**: a Data Scientist in the PEReN, a French government administration which provides an expertise on platform regulation.
- **Kostas Flokos**: CEO at AGEify, an online age verification solution for businesses; and member of the EU euCONSENT ASBL.
- **Onno Hansen-Staszyński**: Independent researcher and consultant; member of an expert group for multiple Dutch Ministries on age verification and harmful content; member of the INT MyData4Children working group; and member of the EU euCONSENT ASBL.
- **Prof. Ross Anderson**: Professor of Security Engineering at the Department of Computer Science and Technology in University of Cambridge.
- **Prof. Sonia Livingstone, OBE**: Professor of Social Psychology and former head of the Department of Media and Communications at the London School of Economics and Political Science; she is a leading British scholar on the subjects of children, media and the Internet.
- **Tony Allen**: Executive Director of Age Check Certification Scheme, a UKAS-accredited conformity assessment body which independently tests and certifies online and offline systems that check age and identity.
- **An anonymous lawyer**: who worked extensively on age assurance.

Via desktop research, we reviewed the relevant legal framework and analysed the available academic papers, civil society organisations reports and regulatory authorities reports on age assurance measures to identify potential associated risks and assess whether the use of these measures could be in tension with the protection of certain fundamental rights.

Based on our findings, we evaluated a wide range age assurance methods following a risk-based approach by assessing the extent to which each method could potentially have a negative impact on fundamental rights, including children's specific rights.

Limitations

Although our evaluation encompasses a wide range of age assurance methods and includes the views of many academics, civil society actors, industry representatives, and regulators, it cannot be considered exhaustive. Our review might have missed some age assurance methods due to the rapid and constant development of digital technologies, as well as relevant views from experts in the field.

We based our assessment on the documentation available for the different methods without performing empirical testing. Our assessment can also differ from those of other relevant stakeholders, including media regulators and data protection authorities who may focus their evaluation on either the reliability or the protection of personal data without including the impact that the assessed age assurance technologies may have on other fundamental rights.

Our mapping of legal requirements for age assurance is limited to European legislation and does not cover the relevant regulatory initiatives at the international or national level. For an broader overview including several jurisdictions around the world, we refer to the Chapter 10 of the Roadmap for age verification from the Australian eSafety Commissioner [31]. Moreover, regarding age assurance requirements associated with the regulation alcoholic beverages, tobacco products and gambling services, as well as the implementation of the Audiovisual Media Service Directive (the AVMSD) in national legal orders, we refer to the study report from Cansu Caglar and Prof. Abhilash Nair, in particular the Chart 2 in point 6.2., published in the context of the euConsent project [15].

Finally, in a few instances, we briefly mention potential alternatives to age assurance measures. Nevertheless, further research is needed to assess the impact of these alternative measures on the protection of both children and adult users in online services.

Definitions

Throughout this study, we adhere to the following terminology:

- **Age assurance** is an umbrella term for both age verification and age estimation solutions. The word "assurance" refers to the varying levels of certainty that different solutions offer in establishing an age or age range [100].
- **Age declaration** means confirming a user's age by requesting them, or another person, to declare the user's age, age-range, date of birth or whether they are above a certain age-threshold (e.g., over 18 years old).
- **Age verification** means a any measure designed to verify the exact age of users of a regulated service [119].
- **Age estimation** means any measure designed to estimate the age or age-range of users of a regulated service [119].
- **Age gate** means a technical measure used to restrict or block access for users that do not meet an age requirement [1].
- **Child** means every human being below the age of eighteen years [121].

1. AGE ASSURANCE, DECLARATION, ESTIMATION, VERIFICATION?

When talking about verifying or estimating someone's age online, terms such as "age verification", "age assurance" ,"age declaration", "age estimation", or even "age assessment" are often used. Within European legislation, the AVMSD, the Digital Services Act (the DSA) and the CSAR proposal all refer to "age verification". The CSAR proposal also mentions "age assessment" measures. Nevertheless, there is currently no definition of those terms under European Law. The level of reliability with which users' age should be established, as well as the methods to be used, are, hence, unclear. For the sake of this study, we will mostly refer to the terms "age assurance", "age declaration", "age estimation" and "age verification", relying on the definitions provided under the UK Online Safety Act 2023 but also reports, standards and position papers from various stakeholders (i.e., ICO, EDRi, 5Rights Foundations and IEEE).

Generally, "*age assurance*" is used as an umbrella term which refers to both "age verification" and "age estimation" or "age assessment" solutions [119]. The word "assurance" refers to the varying levels of certainty that different solutions offer in establishing an age or age range [1]. Consequently, within the study, age assurance refers to any measures able to establish a user's age, irrespective of the measure's level of certainty. Age assurance, therefore, encompasses simple age declarations (i.e., a person simply stating it's age or date of birth, without further verification), age estimation or age assessment, and official document-based age verification. Additionally, according to the Information Commissioner's Office's (the ICO), age assurance may also encompass measures to prevent children from accessing adult, harmful or otherwise inappropriate content when using ISS, without necessary verifying users' age itself [55].

"*Age declaration*" refers to measures requesting users to confirm their age by declaring how old they are, but without providing further evidence of their claim. They can either disclose their age (e.g., "I'm 31 years old"), their age-range (e.g., "I'm between 18-25 years old"), their exact date of birth (e.g., "I'm born on the 19/10/2003"), or declare that they are above a certain age-threshold (e.g., "I'm over 18 years old"). Besides, the declaration can also be made by someone else than the user themselves, for example a parent (parental authorisation) or another user (vouching mechanism). The declaration will then condition the access to certain services or content or enable certain special features depending on the age or age-range disclosed. Finally, some argued that, if a provider states in its terms of conditions that the service is only allowed for users above a certain age threshold, users could be considered as implicitly declaring that they are above such age threshold if they accept the terms and conditions [40].

"*Age estimation*" or "*age assessment*" are measures designed to estimate the age or age-range of users of a regulated service [119]. These measures either predict or estimate age with

a lesser level of accuracy, often by algorithmic means, on the basis of the user's behaviour (e.g., via analysis of browser history or profiling) or by the processing of physical or mental features (e.g., biometric analysis, psychological or cognitive tests) [55]. The outputs, thus, vary from a binary determination as to whether someone is or is not an adult, through to placing an individual in an age category [55]. The 5Rights Foundation, therefore, describes age estimation as "a process that establishes a user is likely to be of a certain age, fall within an age range, or is over or under a certain age. Age estimation methods include automated analysis of behavioural and environmental data; comparing the way a user interacts with a device or with other users of the same age; metrics derived from motion analysis; or testing the user's capacity or knowledge" [1].

Finally, "*age verification*" implies measures which determine a person's age with a high level of certainty by checking against trusted, verifiable records of data [55]. The UK Online Safety Act 2023 defines age verification as "any measure designed to verify the exact age of users of a regulated service" [119]. Verifying the exact age may often require the provision of an official document establishing a date of birth. Consequently, the 5Rights Foundation defines age verification as "a system that relies on hard (physical) identifiers and/or verified sources of identification that provide a high degree of certainty in determining the age of a user. It can establish the identity of a user but can also be used to establish age only" [1]. This definition was also used for the IEEE Standard for an Age Appropriate Digital Services Framework [100]. The European Digital Rights advocacy group (EDRi) even refer to "*document-based age verification*" to highlight the reliance of the method on official identity document, or other age-restricted document, which need to be checked manually or automatically, either by a provider, a government system (e.g. eID) or a third party [40].

2. LEGAL REQUIREMENTS FOR AGE ASSURANCE UNDER EUROPEAN LAW

Although the EU legislator acknowledged in multiple occasions that age assurance, and more particularly age verification, could potentially reduce the risks of children's harm online, there is currently no mandatory requirement, under European law, which would compel providers of information society services (ISS) [111] to verify or estimate the age of their users. However, the Regulation laying down rules to prevent and combat child sexual abuse (CSAR) could, if adopted, introduce such obligation for providers of interpersonal communications services (e.g., Whats' App, Zoom, or a video game's chat) and software application stores (i.e., app stores such as Google Play Store, Apple Store, or Steam). Under the CSAR, these providers would be forced to implement age verification or age assessment measures any time there is a risk for their services to be used for the purpose of the solicitation of children (also referred to as "grooming"). This section will provide a concise overview of the relevant legal provisions related to age verification in the current European legal framework as well as further discuss the implications of the CSAR regarding age assurance requirements.

2.1. General Data Protection Regulation (GDPR)

Regulation 2016/679 (GDPR) provides an harmonised framework for the protection of natural persons, in particular regarding their fundamental rights, in relation to the processing of personal data [112]. Among the natural persons protected under the GDPR, children merit specific protection as they may be aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data (recital 38).

Consequently, *article 8 GDPR* provides that, when based on consent, the processing of the personal data of a child, in relation to ISS offered directly to that child, shall be lawful only if the child is at least 16 years old, or if the consent is given or authorised by the holder of parental responsibility over the child. Member States of the EU can, nonetheless, reduce the age threshold for consent to a minimum of 13 years. If a child gives consent, in the absence of parental authorisation, this consent would, therefore be invalid and the processing of their personal data unlawful [36]. Additionally, article 8(2) GDPR provides that, in such cases, controllers shall make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

Hence, to comply with article 8 GDPR, controllers may rely on age verification although this measure is not even mentioned in the GDPR. As acknowledged by the EDPB in its guidelines 05/2020 on "Consent", the need to undertake reasonable efforts to verify age is not explicit in the GDPR, but is implicitly required [36]. Data protection authorities (DPA) take the implementation of age verification into account when assessing data controllers' compliance

with their obligations under the GDPR, notably vis-à-vis articles 24 and 25 of the Regulation, which respectively require data controllers to be able to demonstrate their compliance with the Regulation (article 24) and implement appropriate technical and organisational measures to ensure the respect of the principles of data protection by design and default (article 25). Accordingly, the Italian DPA (Guarante) decided to temporarily ban OpenAI's and Luka Inc.'s AI-based chatbots "ChatGPT" [8] and "Replika" [52], notably due to their lack of age verification [46,47].

> **Alexandra Zeeb-Schwanhäußer (BfDI)**: "*Under article 8 GDPR, controllers may need to check whether the user is a child to know if they need to rely on parental consent. Art. 8(2) indeed explicitly states that controllers shall make reasonable efforts to assess whether the consent is given or authorised by the holder of the parental responsibility over the child. It could be understood that these reasonable efforts may encompass age assurance measures*."

The necessity to implement age verification measures to comply with GDPR is, however, still debated. In Ireland, the Irish Data Protection Commission (DPC) fined TikTok of €345 million [23,26], after a binding decision from the European Data Protection Board (EDPB) which expressed serious doubts on the "appropriateness" of the age gate implemented by the platform since the measure could be easily circumvented by declaring an incorrect birth date [28,79]. Nevertheless, despite EDPB's views, the decision of the Irish DPC did not conclude that the age gate deployed by TikTok infringed the GDPR and endorsed TikTok's argument that age verification based on hard identifiers would be a disproportionate measure [26,79]. Additionally, the DPC emphasise that relying on hard identifiers could exclude children who - despite being over 13 years old (required age to access TikTok) - could not access such documents [26,79].

As highlighted by both the ICO and the CNIL, the reliance on age verification should be depend on the type of service and the specific circumstances in which it is provided, notably in relation to the risks they may poses to children users [19,55]. In some cases, age assurance may not even be needed. For example, for services which are specifically targeted at children, such as YouTube Kids. For those types of services, it can be reasonably assumed that a significant part of the recipients of their service are children. Therefore, the providers of those services can, either, refrain from collecting personal data, or, request parental consent as a default measure, irrespective of whether the user is actually a child or not. Nevertheless, in other situations, such as mixed-audience services where both children and adults are accessing the service (e.g., video games or social media), age assurance may be relevant to distinguish children users from adults, so that providers request parental consent before processing personal data and, eventually, enable age-appropriate designs.

Besides, as age assurances technologies require the processing of personal data, their use should always remain proportionate to the nature and risks of the service or content they are associated with, as well as the risks associated with processing activities required for verifying or estimating age [19]. This means that if less intrusive measures are available to effectively achieve the objective of protecting children, those measures should be prioritised

(for examples of alternative protective measures, see those listed in the Article 29 Data Protection Working Party's Opinion 5/2009 on Online Social Networking [10] and article 35 of the Digital Service Act [116]).

Where there are sufficient risks to justify the need of age assurance, the level of reliability of the age assurance should depend on the level of severity of the risks associated with the provided service. Indeed, the more precise and reliable, the more invasive and risky the age check will be. For example, age verification measures provide a high degree of certainty regarding a user's age. However, as these measures mostly rely on the provision of an official document, they allow for the identification of the user which can lead to profiling or identity theft. Therefore, only services creating significant risks for children users should justify the reliance on these type of age assurance measures, while less-risky services may rather require users to simply disclose their age, without the need for further verification [36,55]. Indeed, as recognized by the EDPB, the implementation of age assurance technologies should not lead to excessive data processing [36]. Consequently, the data collected for age assurance purpose should be limited to what is strictly necessary and should not be used for other purpose (e.g., commercial purpose) [19].

Finally, age assurance processing shall respect all the data protection principles laid down in *article 5 GDPR*:

- **Lawfulness**: ISS' providers who collect personal data for age assurance purpose shall rely on adequate legal basis. For example, complying with a legal obligation (art. 6 (c) GDPR) such as preventing children from accessing pornography, concluding a contract for which children do not have the legal capacity (art. 6 (b) GDPR), or based on their legitimate interest (art. 6 (f) GDPR) such as establishing that the user is a child to adapt their service accordingly.
- **Fairness**: Any processing of personal data for age assurance must not be detrimental or misleading and no user should be discriminated against. Hence, providers of ISS using age assurance are expected to take action to scrutinise and minimise any potential bias in their approach to age assurance [55].
- **Transparency**: They should also provide users with clear information about why there is a need for age assurance and how the user's age is being verified: what data are collected, whether third parties are involved in the age check and who are they, if the data will be retained and for how long, and what are the user's rights regarding the personal data
- **Purpose limitation**: The data collected for age assurance purpose shall not be further processed for other purposes, especially for commercial purposes [19,53]. The commercial re-use of personal data of minors collected for the purpose of age verification is also prohibited under article 6a of the AVSMD.
- **Data Minimisation & Storage limitation**: Age assurance systems should only collect information which are strictly necessary for establishing the user's age and not retain these once the age assurance has been completed [19]

- **Accuracy**: The accuracy of the age assurance data shall also be guaranteed to prevent false positives (children labelled as adults) and negatives (adults labelled as children) [55]. Although the degree of certainty regarding the user's age shall depend on the level of risks associated with the provided service. Verifying the user's age with precision may indeed result in privacy intrusions which may be disproportionate regarding the risks associated with the provided service [19].
- **Integrity and Confidentiality**: ISS' providers shall also ensure that they use secure age assurance systems and that they handle the age assurance data in a responsible manner to preserve the integrity and confidentiality of the collected data
- **Accountability**: ISS' providers should be responsible for, and be able to demonstrate compliance with the law by documenting their data practices and making them available, when needed, to data protection authorities or certification bodies

2.2. Audiovisual Media Service Directive (AVMSD)

Directive 2018/1808 (AVMSD) regulates both linear and non-linear audiovisual media services (i.e., TV and radio broadcasts, videos on-demand, and video-sharing platforms) [113].

Article 6 (a) AVMSD specifically targets children's exposure to harmful content by requiring that Member States of the European Union to take appropriate measures to ensure that audiovisual media services provided by media service providers under their jurisdiction which may impair the physical, mental or moral development of minors are only made available in such a way as to ensure that minors will not normally hear or see them. Among the potential preventive measures, the article specifically mentions age verification tools.

Article 28 (b) of AVMSD provides a similar obligation for Member States regarding the programmes, user generated videos and audiovisual commercial communications provided on video-sharing platforms. The paragraph 3 of this article lists 10 measures to prevent exposure to harmful content, as appropriate. Among these measures, age verification tools are specifically mentioned, in point (f), with respect to content which may impair the physical, mental or moral development of minors. The end of this paragraph also specifically prohibits to re-use personal data of minors, collected or otherwise generated by video-sharing platform providers to verify the user's age (point (f)) or enable parental controls (point (h)), for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising.

The AVMSD thus suggests age verification tools as an appropriate measure to prevent children accessing audiovisual content which can be detrimental to them. However, it does not mandate it. Age verification tools are only an option among others (e.g., parental controls (point (h)), age rating systems (g)), or reporting mechanisms (points (d) and (e))). Their implementation should, hence, depend on the type of content and the circumstances in which it is provided. Both article 6 (a) and 28 (b) provide that the preventive measures shall be proportionate to the potential harm of the content.

Consequently, the appropriate measures shall be determined in light of the nature of the content in question, the harm it may cause, the characteristics of the category of persons to be protected as well as the rights and legitimate interests at stake (including those of media service providers, users generating the content, and the general public). Therefore, not all content should be subject to age verification. Only the most harmful content, such as gratuitous violence and pornography, shall be subject to the strictest measures.

Except when age verification is specifically mandated by law (e.g. pornography under certain jurisdictions), media service providers should, hence, adopt a risk-based approach when assessing the need for age verification measures and the level of accuracy required in determining a user's age. Similarly, once they identify a user's age, media service providers should also consider the risks associated with the specific content they provide when deciding how to appropriately protect the child user, taking into account its age range. A strict access prevention might indeed be disproportionate, depending on the circumstances, and other less restrictive protective measures may be more appropriate. Moreover, when conducting those risk assessments, media service providers shall consider the full scope of rights of all users seeking access to their content, including the rights to freedom of expression, access to information, protection of privacy and personal data, and non-discrimination.

Media service providers may, however, face challenges in implementing this risk-based approach. Indeed, as a directive, the AVMSD merely provides minimum requirements allowing Member States to further define the types of content deemed harmful and the adequate measures to restrict their access. Due to cultural differences in the perception of the risks associated with specific content for particular age groups, the selection of the appropriate protective measures may vary across jurisdictions [15]. Additionally, children and regulators may have different views regarding what constitutes harmful content. For example, the children's access to certain content, such as animal suffering, may not be considered as unlawful, although children may consider such content as significantly harmful.

As a result, it might be difficult for media service providers to rely on a single pan-European solution that would fit all national contexts. Member states may have different national requirements which can lead to an unequal deployment of age assurance tools in the European digital environment. Moreover, the current lack of specific guidance on how to implement age assurance tools in practice, creates uncertainties regarding the trustworthiness of age assurance solutions.

2.3. Digital Services Act (DSA)

Regulation 2022/2065 (DSA) aims to ensure a safe, predictable and trusted online environment by harmonising rules in the provision of intermediary services, notably via specific due diligence obligations (art. 1 DSA) [116]. Section 3 of chapter III specifies the obligations of providers of online platforms, in particular regarding the protection of minors.

Article 28 DSA provides that:

> *"1. Providers of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service. 2. Providers of online platforms shall not present advertising on their interface based on profiling within the meaning of Article 4, point (4) GDPR using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor. 3. Compliance with the obligations set out in this Article shall not oblige providers of online platforms to process additional personal data in order to assess whether the recipient of the service is a minor. 4. The Commission, after consulting the Board, may issue guidance to assist providers of online platforms in the application of paragraph 1."*

To comply with the first two paragraphs of this article, providers of online platforms, which are accessible to minors, may be tempted to rely on age assurance measures. Such measures could indeed ensure that they distinguish minors from adults and thus adapt their services to the former's specific needs for high level of privacy, safety and security (§1), and absence of targeted advertising based on profiling (§2).

However, the DSA explicitly states, in art. 28(3) and recital 71, that age verification is not an obligation and warns providers of online platforms to refrain from processing additional personal data in order to assess whether the recipient of the service is a minor, pursuant to the GDPR's principle of data minimisation. Recital 71 further emphasises that the prohibition of displaying targeted advertising to children "*should not incentivise providers of online platforms to collect the age of the recipient of the service prior to their use*." The same recital, instead, recommends to design, where appropriate, online interfaces with default settings ensuring the highest level of privacy, safety and security for minors, as well as following age-appropriate standards and code of conducts.

By contrast, article 35(1), point (j) specifically mentions age verification as an appropriate targeted measure to protect the rights of the child from the systemic risks stemming from the design or functioning of very large online platforms (VLOPs) and very large online search engines (VLOSEs) and their related systems. Providers of VLOPs and VLOSEs - which are online platforms and online search engines with a minimum of 45 millions average monthly active users in the EU and are designated by the Commission. Among VLOPs, the Commission already designated services such as Google Play, Apple AppStore, Instagram, Facebook, Snapchat, TikTok, or Youtube, and recently added, on 20 December 2023, three providers of pornographic websites, namely Pornhub, Stripchat and XVideos. These VLOPs may, therefore, rely on age verification to comply with their risk mitigation obligation under article 35(1) of the DSA.

This article, however, explicitly states that the implemented mitigation measures shall be reasonable, proportionate, effective, and tailored to the specific systemic risks, with particular

consideration to the impacts of such measures on fundamental rights. Consequently, before implementing age verification measures, providers of VLOPs and VLOSEs should assess the risks associated with such implementation, in particular regarding the protection of the fundamental rights. Additionally, if other mitigation measures (including those listed in article 35) which are less restrictive than age verification are available, providers of VLOPs and VLOSEs should prefer such measures, pursuant to the principle of proportionality. Therefore, alongside age verification, providers of VLOPs and VLOSEs should also consider parental controls tools or tools aimed at helping minors signal abuse or obtain support, but also implementing age-appropriate designs (point (a)), adapting the content moderation processes (point (c)) and recommender systems (point (d)), limited or adjusting the presentation of advertisements (point (e)), or initiating or adjusting cooperation with trusted flaggers in accordance with article 22 of the DSA (point (g)).

2.4. Proposed Regulation on Child Sexual Abuse (CSAR Proposal)

2.4.1. Objectives and Controversies

Introduced by the European Commission in May 2022, the proposal for a Regulation laying down rules to prevent and combat child sexual abuse (also know as the CSAR proposal) aims to impose new obligations to providers of relevant ISS, as well as providers of internet access services, concerning the detection, reporting, removing and blocking of known and new online child sexual abuse material (CSAM) and solicitation of children (also referred to as "grooming") [115].

The proposal, however, faced strong criticisms, notably for its lack of proportionality and privacy intrusiveness. Although, the objectives pursued by the Commission is undoubtedly noble, protecting children from online sexual abuse should not lead to the annihilation of the confidentiality of private communication which is pivotal for a democratic society. Section 2 of the proposal, indeed, introduced detection obligations requiring providers of hosting services and providers of interpersonal communications services to automatically scan their user's private communications within their services to detect potential online child sexual abuse, where one of the users is a child user (meaning someone below 17 years old) [12]. Many, including the EDPB and EDPS, argued that such obligation would heavily jeopardise end-to-end encryption, affecting the confidentiality of private communication, and seriously undermining the very essence of the right to privacy and data protection, enshrined in article 7 and 8 of the Charter of the Fundamental Rights of the European Union (CFREU) [37].

Additionally, the European Commission, in particular the Department of the Home Affairs under Commissioner Ylva Johansson who initiated the proposal, is currently under scrutiny to determine whether it broke the recently introduced DSA's rules on micro targeted political advertising campaigns. The Department was, indeed, found running a paid advertising campaign on the social media X (formerly Twitter) to promote the CSAR proposal towards targeted users in countries which did not support the proposal in the Council's discussions

(i.e., Netherlands, Sweden, Belgium, Finland, Slovenia, Portugal and the Czech Republic) [70]. This follows previous claims by investigative journalists from BalkanInsight on potential commercial influence over the Home Affairs Commissioner by companies selling CSAR-scanning tools [101].

Consequently, given the backlash faced by the proposal, the discussions within the EU legislative trilogue will certainly be lively. Both the Council and the European Parliament have yet to adopt their positions, which will probably result in a series of amendments. However, in this study, our analysis is restricted to the proposal as introduced by the Commission in May 2022 and focuses on the age verification requirements provided in article 3, 4 and 6 of the proposal.

2.4.2. Scope: Interpersonal Communications & App Stores

Among relevant ISS, the proposed regulation notably covers providers of interpersonal communications services as well as providers of software application stores.

On the one hand, *interpersonal communications services* means:

> "*any publicly available service, normally provided for remuneration, that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s), including services which enable direct interpersonal and interactive exchange of information merely as a minor ancillary feature that is intrinsically linked to another service*" - art 2 (b) of the CSAR proposal.

Interpersonal communications services, therefore, cover instant messaging apps, such as Whats' App, Telegram, Signal or Messenger, but also online meeting apps such as Zoom or Microsoft Teams, as well as any private channels integrated any type of service (e.g., a private chat in a video games).

On the other hand, *software application stores* concerns:

> *ISS which provide a online intermediation service between business users offering any digital product or service that runs on an operating system (i.e., software applications) and the consumers to which those product or services are offered, with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded* (see, art. 2(d) of the CSAR proposal and art. 2 (5),(14),(15) of Regulation 2022/1925 (DMA))

In simpler terms, software application stores are often referred to as "App Stores." They include services such as Google Play Store, Apple Store, but also other types of platforms

such as Steam (for video games) or to a certain Amazon (when the product sold is a software application).

Software application stores also qualify as "hosting service" as they meet the definition provided in article 3 (g)(iii) of the DSA. A hosting service consists in the storage of information provided by, and at the request of, the recipient of the service (in this case, the providers of software applications).

Consequently, under those two definitions, a very wide range of ISS fall under the scope of, either, interpersonal communications services, or, software application stores.

2.4.3. Age Verification as a Criterion for Risk Assessment

Among the obligations proposed by the regulation, article 3 requires providers of hosting services (including software application stores) as well as providers of interpersonal communications services to conduct and update *risk assessments* to identify, analyse and assess, for each of their services, the risk of use of such services for the purpose of online child sexual abuse.

Article 3(2) lists several criteria that those providers shall take into account when carrying out such risk assessment. Point (b) of that article specifically mentions the implementation of functionalities enabling age verification as a mean to address the risks of online child sexual abuse.

Additionally, with respect to the risk of solicitation of children for sexual purposes, point (e) emphasises that providers shall take into account the extent to which their services are used or are likely to be used by children (sub-point (i)), and if so, the different age groups of the child users and the risk of solicitation of children in relation to those age groups (sub-point (ii)). Article 3, therefore, builds on the premise that the implementation of age verification would allow providers to identify the proportion of children and adults accessing their services and, consequently, assess the likelihood that their services may be used for the purpose of solicitation of children. While, in the absence of such measure, children and adults users would be indistinguishable, which may increase the risk of grooming.

2.4.4. Age Assurance as an Enabler of Mitigation Measures

Under the CSAR proposal, age verification and age assessment (also known as "age estimation") measures are also considered as enablers for both providers of interpersonal communications services and providers of software application stores to take reasonable mitigation measures to reduce the risk of grooming via their services.

2.4.4.1. Requirements for Interpersonal Communications

Article 4(3) of the proposal, indeed, provides that:

> "*Providers of interpersonal communications services that have identified, pursuant to the risk assessment conducted or updated in accordance to article 3, a risk of use of their services for the purpose of the solicitation of children,* ***shall take the necessary age verification and age assessment measures*** *to reliably identify child users on their services, enabling them to take the mitigation measures*".

Consequently, if providers of interpersonal communications services have identified that there is a risk that their services may be used for the purpose of child solicitation, and that they did not implement age assurance measures yet, they will be compelled, under the CSAR, to implement either age verification or age assessment measures. The rationale for mandating age assurance is that such measures would enable providers to take mitigation measures addressing the risks of child solicitation. Article 4(1) of the CSAR proposal lists potential mitigation measures. Moreover, recital 16 of the proposal suggests that the mitigation measures listed in article 35(1) of the DSA could also be considered if they are relevant to address the risks of online child sexual abuse.

Additionally, providers of interpersonal communication services, who have assessed that their service may have significant risks of solicitation of children and have identified users as children users (e.g., via the age assurance measures mandated under article 4(3)), may eventually received a detection order, pursuant to section 2 of the CSAR proposal, requiring them to scan conversation involving at least one child user. As highlighted by EDRi, this means that providers will keep ongoing records of all their users' ages to ensure they can continuously distinguish child and adult users to comply with detection orders [40].

2.4.4.2. Requirements for Software Application Stores

Article 6(1) provides that:

> *"Providers of software application stores* ***shall***:
>
> *(a) make reasonable efforts to assess, where possible together with the providers of software applications, whether each service offered through the software applications that they intermediate presents a risk of being used for the purpose of the solicitation of children;*
>
> *(b) take reasonable measures to* ***prevent child users from accessing*** *the software applications in relation to which they have identified a significant risk of use of the service concerned for the purpose of the solicitation of children;*
>
> ***(c) take the necessary age verification and age assessment measures to reliably identify child users*** *on their services, enabling them to take the measures referred to in point (b).*"

Under article 6 of the CSAR proposal, providers of software application stores (e.g., App Stores) are, therefore, required to implement age assurance measures for identifying child users but also to prevent them, for instance via age gates, from accessing any app which may eventually be used for the purpose of children solicitation. As developed in the next subsection, such obligations are very likely to be disproportionate and create significant hindrance for the exercise of children's rights in the online environment.

2.4.5. Legal Certainty & Proportionality

Both the provisions of article 4(3) and article 6(1) of the CSAR proposal introduce very broad obligations which could lead providers of interpersonal communications services and providers of software application stores to implement age verification measures by default to ensure compliance.

Under article 6(1)(c), providers of software application stores have no other option than implementing age verification or age assessment measures to enable the access prevention of children users to software applications which could present the risks of being used for the purpose of child solicitation. Among those software applications, some may be interpersonal communications services also subject to the obligation of verifying their user's age, and scan conversations involving children users, if the services are deemed to create the risks mentioned above.

Given that the criteria to evaluate whether there is a "risk of the relevant services being used for the purpose of children solicitation" are quite unclear under the CSAR proposal, the EDPB and the EDPS acknowledged, in their joint opinion 4/2022 on the CSAR proposal, that providers (but also supervisory authorities) in charge of applying the CSAR's obligations enjoy a broad margin of appreciation in determining the existence of such risks [37]. Although introducing a series of interferences with and restrictions to the fundamental rights of natural persons, including the right to privacy and data protection, the CSAR proposal does not provide sufficient clarity regarding when and where those interferences and restrictions are allowed. This leads to legal uncertainty on how to balance the rights at stake in each individual case. Consequently, according to the EDPB and the EDPS, the proposal, in its current form, leaves too much room for potential abuse due to the absence of clear substantive norms [37].

With regard to age verification, providers to ensure compliance with their obligations under the CSAR, may extensively interpret the notion of "risk of their services being used for the purpose of child solicitation" leading to the implementation of age verification almost as a default measure. Although article 4(2) of the proposal provides safeguards to ensure that the mitigation measures, implemented by providers of interpersonal communications services and providers of hosting services (including software application stores), shall be effective (point a), targeted and proportionate in relation to the identified risks (point b) and applied in a diligent and non-discriminatory manner, having due regard, in all circumstances, to the potential consequences of the mitigation measures for the exercise of fundamental rights of all parties affected (point c); there is no sufficient guarantee that those providers conduct

sufficient assessments of the consequences associated with the implementation of age assurance measures, since the CSAR explicitly force them to implement them.

Moreover, the EDPB and EDPS recognized that age assurance measures could lead to privacy intrusion and discrimination [37]. Regarding age verification, there is currently no technological solution that is capable of assessing with certainty the age of a user in an online context, without relying on an official identity document. The provision of such documents, however, reveal more information than needed to establish a user's age, leading to the identification of the user and, thus, creating unnecessary risks for the protection of users' fundamental rights, which can inhibit or discourage the legitimate use of the affected services. Additionally, mandating age verification for online services would lead to the exclusion of undocumented persons who do not have access to the verified age credentials. Similarly, if the age verification measures rely on the provision of a digital identity, such as an eID, it will prevent access to European citizens who are nationals of Member States where such identities are not available. Concerning age estimation, the reliance of the associated technologies on the processing of either biometric or behavioural data raises significant data protection concerns. Moreover, the remaining challenges concerning the accuracy and error rates of those technologies may lead to unacceptable discrimination. The EDPB and EDPS, therefore, recommends to amend CSAR proposal provisions to expressly allow providers to rely on parental control mechanisms in addition or as an alternative to age verification.

We share the EDPB and EDPS' concerns regarding the interferences that age assurance measures create with the fundamental rights of natural persons. Therefore, we recommend the European legislator to repeal the mandatory requirements for age assurance measures, provided under articles 4 and 6 of the CSAR proposal. Moreover, we suggest to make it explicit that the safeguards provided under article 4(2) apply to the implementation of age assurance measures.

We also want to highlight that restricting children users' access to a wide-range of online services, as provided under article 6(1)(b), may significantly impact the exercise of their rights protected under the United Nations Convention on the rights of the child (UNCRC), notably their rights to access appropriate information (art. 17 UNCRC), to express their views (art. 13 UNCRC), to associate with one another (art. 15 UNCRC), to access education (art. 28 UNCRC), to play (art. 31 UNCRC), or to simply develop their skills in the digital environment (art. 6 UNCRC).Given the broad margin of appreciation of provider of software application stores regarding the potential existence of risks of grooming on the software applications they intermediate, it is likely that children will be prevented from accessing a wide range of software applications from which they could benefit from (e.g., social media, video-games, or encrypted private messaging apps). When complying with their obligations under the CSAR, providers of software application stores should, therefore, take into primary consideration the best interest of the child, by assessing the impact that the access prevention may have on the affected children, and balancing the protection of children with their empowerment vis-à-vis the exercise of their rights. Consequently, providers should only prevent children users from accessing their apps, when there is a serious risk of child solicitation which would justify that the protective restriction of access overrides the exercise of children's rights via the use of these apps.

Finally, pursuant to the principle of proportionality, we recommend ISS providers to refrain from implementing age assurance measures if appropriate alternative mitigation measures, which are less restrictive of users' fundamental rights, are available. In such instances, such measures could be applied, where appropriate, to all users, irrespective of their age. Those alternative measures, for example, encompass adapting the content moderation and/or recommendation systems, enabling by default warnings before displaying risky content, making accessible a panic button to provide victims with quick and effective support, and ensuring effective and easy-to-use reporting and compliant mechanisms.

2.5. Adopting a Risk-Based Approach

2.5.1. Necessity and Proportionality Principles

All the European legislations discussed above underscore the importance of implementing age assurance measures in accordance with the principles of necessity and proportionality. The GDPR emphasises the principle of data minimization (Article 5(c) GDPR), requiring data controllers to limit processing to what is strictly necessary for the purpose of age verification. Additionally, to ensure fair processing (Article 5(a) GDPR) and default protection of data subject rights (Article 25 GDPR), controllers must implement suitable technical and organisational measures, considering the risks to the rights and freedoms of individuals (Article 24 GDPR). This may include conducting a data protection impact assessment, pursuant to article 35 GDPR.

In the context of the AVSMD, both articles 6(a) and 28(b) state that measures to prevent children from being exposed to harmful content must be proportionate to the potential harm. Similarly, article 35 of the DSA explicitly mandates mitigation measures that are reasonable, proportionate, effective, and tailored to specific systemic risks, with a particular focus on their impact on fundamental rights.

Lastly, the CSAR proposal mandates age verification under certain circumstances. However, article 4(2) of the proposal emphasizes that measures to address online child sexual abuse must be effective, targeted, proportionate to identified risks, and applied diligently and non-discriminatory manner, considering the potential consequences for the exercise of fundamental rights of all parties affected.

All these requirements derive from the application of Article 52(1) of the CFREU, allowing limitations to protected fundamental rights under strict conditions. Limitations must be provided for by law, respect the essence of the rights and freedoms, be necessary and genuinely meet objectives of general interest or the need to protect the rights and freedoms of others. This implies that measures restricting fundamental rights should be justified by legitimate objectives, be effective in achieving those objectives, and subject to the principle of proportionality, ensuring that negative consequences do not outweigh the benefits associated with achieving legitimate objectives and that no less restrictive alternative measures are available.

Consequently, age assurance measures should only be implemented when strictly necessary, following a risk-based approach [37]. Hence, ISS providers should have due regards to the specific circumstances in which children may access the provided service, or certain of its features, as well as the consequences of such access for children's well-being. Via the performance of impact assessments (see Section **2.5.2.**), ISS providers should determine the need for age assurance measures, as well as the level of reliability of the proof of age, striking a fair balance between the risks associated with the child's access to their service and those stemming from the age assurance measures they may consider to implement to prevent such access. If the provider considered that age assurance is needed, the choice of the methods available to users should also be based on an evaluation of the specific risks associated with each method, e.g. privacy, security or discrimination related risks (see Section **4**). Providers should ensure that appropriate mitigation measures are implemented to minimise these risks as much as possible. When the access to the service, or certain of its features, is conditioned to age assurance, providers should identify the impact, notably regarding the exercises of certain fundamental rights, that a restriction decision may have on users who are prevented from access (including users whose age may have been wrongly estimated). Finally, to ensure adherence to the principle of proportionality, providers must assess whether the negative consequences of implemented age assurance measures outweigh the positive outcomes of shielding children from harmful or risky services and content. This assessment should involve a comparison of the potential impact of age assurance measures with that of other effective mitigation strategies.

> **Jen Persson (Defend Digital Me)**: "*Before deciding if there is a need for age verification, it should be determined what actually ARE the tools we are using and for what purpose we want to use them. If children's safety is the end goal, how will you measure that? What's your success rate? Why adopt this method for trying to solve this problem if you don't even know how you'll measure whether it worked or not.*"
>
> **Sonia Livingstone (London School of Economics)**: "*If a child says 'I'm a child' and then the service swung into place in an effort to protect their rights, positive and negative, how much of the problem would be solved that way? You might identify the child as a 12 years old, but then the question is what happens next? The age assurance just tells the person's age, this is not where decision-making to restrict access is made. This rather depends either on use of parental controls, service providers' internal rules, or regulation*."
>
> **Duncan McCann (5Rights Foundation)**: "*The choice of the method is a case by case analysis, which depends on how robust you want the age check to be, depending on the level of the associated risks.*"

2.5.2. Performing Fundamental Rights Impact Assessments (FRIA)

Providers should conduct impact assessments to evaluate the risks associated with implementing age assurance measures on the fundamental rights of all individuals who may be affected, regardless of age or whether they are recipients of the provider's services. These assessments should extend beyond privacy and data protection rights, encompassing all fundamental rights protected under the Universal Declaration of Human Rights (UDHR) [122], the European Convention on Human Rights (ECHR) [103], and the Charter of Fundamental Rights of the European Union (CFREU) [117], as well as the specific rights of children outlined in the United Nations Convention on the Rights of the Child (UNCRC) [121]. Providers implementing age assurance measures should, therefore, conduct fundamental rights impact assessments (FRIA), which include both data protection impact assessments (DPIA) and children's rights impact assessments (CRIA).

In this study, we identify a series of risks stemming from the implementation of age assurance measures and link them to the fundamental rights they may impact. We also assess how different age assurance methods influence the likelihood of these risks occurring and the severity of their impact on the fundamental rights of individuals.

3. RISKS AND TENSIONS WITH FUNDAMENTAL RIGHTS

As an initial point, it is essential to underscore that the probability of the risks detailed below as well as the severity of their impact on individual fundamental rights depend on the type of age assurance measures implemented and the specific contexts in which these measures are deployed. Key factors, such as the nature of the provided services or content and the type of the service provider (private company, governmental agency, NGO, or another entity), play a significant role in shaping the associated risks.

Likewise, the kind of services or content offered and the circumstances of their delivery can influence the nature of the data collected from users, particularly in terms of its sensitivity (e.g., potential or actual indications of sexual orientations, especially relevant in the context of adult websites). The impact on users may also vary based on the type of services or content they are denied access to; for example, children may experience different effects when restricted from accessing a pornographic website, a social media platform, an instant messaging app, or a video game.

Given these considerations, it is imperative to assess the outlined risks while taking into account the unique circumstances of each scenario. Evaluating these risks, therefore, requires a meticulous case-by-case analysis.

3.1. Identifying Users

The primary and substantial risk associated with age assurance, particularly in document-based age verification but also certain age estimation methods (e.g. facial scans), lies in the potential identification of the service recipient. If these methods fail to anonymize personal data and retain information longer than necessary, they pose a significant risk of privacy intrusion. Connecting users' identities with their service usage may reveal highly sensitive personal information and lead to a loss of online anonymity. Moreover, the gathered information may be utilised for purposes beyond age assurance, such as commercial profiling or government surveillance. Finally, in the absence of sufficient security, the data collected for could potentially be leaked and/or misused by malicious actors. In that regard, the processing of biometric data raises significant concerns. A widespread implementation of online age assurance measures would, therefore, substantially increase the risks of identity theft and data fraud.

3.1.1. Privacy Intrusion

The identification of users through age assurance systems may be excessively invasive, revealing more information than necessary for establishing a user's age. This practice introduces a range of risks applicable to all users, regardless of their age, and these risks often outweigh the potential benefits. Associating a user's online activities with their identity can, for example, expose highly sensitive information, depending on the nature of the provided service. For instance, on a pornographic website, user identification may disclose details such as who is accessing the service, the specific video categories they watch (indicating presumed or actual sexual orientation), average time spent on the site, and frequency of visits providing insights into potential patterns related to mental or physical health, such as potential addiction to pornography. It can even unveil when and potentially from where users access the website, potentially indicating whether they are consuming explicit content during working hours. In other contexts, like social media, user identification may also reveal political and philosophical opinions, paving the way for potential political profiling. Age assurance measures can, hence, significantly breach user's right to privacy (art. art. 12 UDHR; art. 8 ECHR; art. 7 CFREU; and art. 16 UNCRC) and data protection (art. 8 CFREU).

Furthermore, concerning age estimation relying on biometric data, such as face scans, previous research has shown that users, including children, tend to favour these measures due to their perceived ease of use. However, it is highly doubtful that users, especially children, fully grasp the potential implications of processing biometric data. The critical question arises: is there sufficient information provided in an age-appropriate manner to enable users to give genuinely informed and freely given consent, particularly when this consent is a prerequisite for accessing the desired service?

Lastly, the widespread adoption of age assurance in the online realm could cultivate a societal habituation to being identified and tracked online. Age assurance measures, particularly those employing face scans for age estimation, might contribute to a broader acceptance of biometric data processing, extending even to routine activities such as accessing a social media platform, playing a video game, or purchasing a meal at a school canteen [99]. The profound societal implications of such habituation are yet to be fully understood.

> **Jen Persson (Defend Digital Me)**: "*We haven't yet grappled with the long term societal implications of the normalisation of showing your face every time for trivial things, as opposed to keeping your facial identity as something that is significant and should be used, for example, in border control. The protection of a face, the protection of an image, should have a much higher value than we are currently assigning it.*"
>
> **Duncan McCann (5Rights Foundation)**: *"If you want to be 100% sure that people are not circumventing the age verification you have implemented, you need to create a very adversarial system to ensure and monitor this, which will rely more and more on surveillance.*"

3.1.2. Loss of Online Anonymity

Age assurance systems, when exposing a user's identity and connecting it to their online actions, pose a significant threat to online anonymity. This loss of anonymity creates a pervasive sense of surveillance, discouraging people from freely expressing themselves, seeking information, or connecting with others online. The resulting chilling effect on legitimate user activities can impede the genuine exercise of fundamental rights, presenting challenges to democratic societies [40].

Beyond societal implications, the consequences of losing online anonymity are particularly grave for certain groups. Individuals such as investigative journalists, activists, human rights defenders, and whistle-blowers rely on anonymity to ensure their safety in both online and offline realms. The absence of anonymity can expose them to harassment, intimidation, and physical harm. Similarly, vulnerable groups like sex workers, marginalized communities, and survivors of child sexual abuse or domestic abuse face an increased risk of violence and exploitation when their identities are known.

3.1.3. User Profiling

The ability to link users' identities to their online behaviour also creates the risk of secondary use of this information for purposes which goes beyond the mere verification of their age, such as profiling users for commercial, policing or political purposes.

3.1.3.1. Commercial Profiling

In today's digital landscape, the predominant business models of companies heavily depend on extensive personal data collection, including from children [49]. This practice facilitates targeted advertising and personalised marketing strategies designed to influence users towards increasing their engagement with providers' services [72]. The wide deployment of age assurance measures in online services may lead to a concentration of users' information in the hands of commercial entities. This could empower these companies to create profiles on the basis of users' age but also on other information revealed during the age assurance process. These intrusive and manipulative practices can have diverse impacts on children, affecting their rights to privacy and data protection (art. 16 UNCRC), impinging on their freedom of thought (art. 14 UNCRC), and exposing them to potential economic exploitation (art. 32 UNCRC) [124]. As outlined by data protection authorities [19,53], providers collecting information from minors for age assurance purpose should not use such information for other purpose such as commercial profiling, direct marketing, and targeted advertising. Such practice is also prohibited by article 6(a) of the AVSMD which is applicable to any media services providers falling under the jurisdiction of a EU Member State. Similarly, article 28(2) of the DSA prohibits providers of online platforms to present targeted advertising to minors. Nevertheless, despite the existing regulation, companies often remain unaccountable due to the challenges related with the effective enforcement of these rules [15,91].

3.1.3.2. Policing and Political Profiling

Upon legal orders, ISS providers may eventually be requested to share users' information with law enforcement authorities for purposes such as combating child sexual abuse, terrorism, or illegal immigration. The extensive implementation of age assurance systems may heighten the risk of state surveillance, particularly impacting marginalised communities and minorities. The data generated through age assurance measures could be exploited to create profiles of individuals based on factors such as origin, ethnicity, religion, sexual orientation, or political opinions. This has the potential to jeopardise fundamental rights if governments target individuals based on these characteristics.

> **An anonymous lawyer**: "*State surveillance risks are very real. We might have a false conception of what an authoritarian regime is and the slippage that might happen, including in European countries. Besides, there is a responsibility even beyond Europe because these companies are likely to roll things out globally so we really need to think about the impact that age assurance measures may have on people in other parts of the world… Sometimes, private companies don't have other options than sharing data with governments to comply with a legal order*."
>
> **Han Hye Jung (Human Rights Watch)**: *"I'm terrified about the potential misuse of this technology to, for example, target children seeking asylum in Europe for the purpose of denying them their rights.*"

3.2. Data Leakage

The concentration of users' information in the hands of service providers, whether they are providers of requested services or age assurance solutions, inherently amplifies the risk of personal data leaks. In instances where security measures are insufficient, malicious actors can exploit vulnerabilities in systems to gain access to users' identities. This unauthorised access can open the door to various forms of misuse, potentially resulting in significant harm to individuals. Alternatively, age assurance measures may also be used to disguise phishing attacks. For example, implementing age assurance measures on a fake website to steal users' personal data by requesting them to upload official document, credit cards or scan their face or fingerprints.

3.2.1. Victim Targeting

When malicious actors gain access to stolen information about users, they can meticulously identify potential victims and tailor deceptive techniques for scams, blackmails, phishing attacks, or grooming. This customization allows for more convincing and targeted schemes, therefore, increasing the likelihood of success. In scams, personalised details make fraudulent scenarios more appealing and harder for targeted victims to discern. Blackmail becomes a potent threat as intimate information (e.g., user's history from a porn websites) empowers coercion, leading to severe emotional distress for victims. In phishing attacks, tailored messages exploiting specific interests heighten the risk of individuals falling for

deception. Finally, personalised grooming enables sexual predators to exploit detailed information to manipulate emotions and trust of their victims more effectively, especially if they are children. The customization of malicious tactics based on stolen user data, hence, significantly aggravate potential harm, threatening individuals' security, and posing risks for physical and mental well-being.

3.2.2. Identity Theft

When users' information leaks, there's a substantial risk of identity theft as malicious actors may impersonate or create deceptive content, such as deep fakes, using the stolen data (e.g., ID card and photos of faces). The stolen identities may also be exploited for fraudulent activities, creating a profound and troubling impact on the victim's well-being. Beyond the harm to reputation, this breach can cause severe emotional distress and mental health implications for individuals affected.

> **Tony Allen (Age Check Certification Scheme)**: "*Identity theft is clearly a risk of misuse. The difficulty is that there is nothing to stop somebody setting up a website… I mean, we haven't seen any evidence of that happening to be fair, but it is possible that it could happen. If consumers aren't aware of the need to check for phishing attacks, then they could be at risk. However, this is already happening in many websites, so the risk is not specific to age verification, but age verification could be used as a cover for phishing attacks.*"

3.2.3. Data Fraud

As pointed out by the CNIL, utilising payment card validation for age verification introduces the risk of phishing attacks [20]. In the event that unauthorised parties acquire personal information, such as credit card details or login credentials, they may exploit this data for unauthorised transactions, resulting in tangible financial losses and potential damage to individuals' credit histories. Additionally, the heightened risk of phishing attacks is a worrisome outcome. Exploiting the compromised information, malicious actors can deceive individuals into revealing even more sensitive details, establishing a troubling cycle of fraud. The repercussions extend beyond immediate financial harm, leaving victims to grapple with enduring consequences, impacting their financial stability and fostering a sense of vulnerability and mistrust.

> **Joris Duguépéroux (PEReN)**: "*Depending on the kind of method used, we could imagine leaks of users' identity cards, photos of faces, bank account numbers, or credit card details. If possible, we would like to avoid this information to be retained after the age check to prevent such leaks.*"

3.3. Hindering the Legitimate Use of Digital Technologies

3.3.1. Restricting Autonomy and Fundamental Rights

Age assurance measures significantly impairs individuals' autonomy online as they create cumbersome barriers to the free exercise of legitimate online activities. In today's society, online services such as social media, interpersonal communication services, video-sharing platforms, or even video games, play a crucial role in exercising individual fundamental rights and contributing to society. These services allow people to express themselves; access information, education, and entertainment; connect with each other; and develop their skills and knowledge.

Conditioning the access to these services to the age assurance, therefore, not only forces users to surrender personal data and compromise their privacy but also creates significant risks that individuals, both adults and children, are prevented from the legitimate exercises of their fundamental rights through their online activities. In the U.S., several state legislations mandating age verification are notably facing legal challenges, asserting that they infringe upon free speech protected by the First Amendment of the U.S. Constitution [48].

> **Jen Persson (Defend Digital Me)**: *"Age verification builds in this assumption that we're talking about children when in fact this is a debate about a layer of technology that creates a lens through which the Internet can be accessed or can be viewed [by all], and it affects everybody who uses the Internet or wants to access or view content."*

Consequently, depending on the type of services for which they are deployed, age assurance measures may impair the exercise of the right to freedom of expression (art. 19 UDHR; art. 10 ECHR; art. 11 CFREU; and art. 12-13 UNCRC); right to access to information (art. 11 CFREU; and art. 17 UNCRC), right to education (art. 26 UDHR; art. 14 CFREU; and art. 28 UNCRC), right of children to leisure and entertainment (art. 31 UNCRC), and right to freedom of association (art. 20 UDHR; art. 11 ECHR; art. 12 CFREU; art. 15 UNCRC). Their implementation should, hence, be conditioned to the performance of adequate necessity and proportionality assessments, taking the best interest of the child as a primary consideration (art. 3 UNCRC).

3.3.2. Risk of Over-Restriction and Censorship

Due to varying cultural norms and national regulations, the lack of a universal standard for what is deemed suitable for children places the onus on service providers to determine where age assurance measure is needed. While certain services like gambling or pornography are widely agreed to be for inappropriate children, defining appropriateness remains challenging, resulting in varied perspectives within the European Union and globally [15]. Hence, providers may be incentivised to align with the strictest standards to ensure compliance with the whole range of legal requirements. This may lead to excessively restricting children's

online experiences, preventing their access to lawful content such as topics related to certain communities (e.g., LGBTQI+), social protestations, or controversial issues [40]. For example, relevant information on sex and sexuality education, sexual health information, and reproductive healthcare may be subject to age assurance. In Germany, the youth protection filter "Jusprog" was found to block access to websites related to contraception, coming out, and suicide prevention [74]. Such information is, however, crucial for children to develop themselves safely and ensure both their physical and mental health. Imposing age verification requirements on individuals seeking access to this content may thereby hinders both children's right to access information (art. 17 UNCRC) and right to health (art. 24 UNCRC).

Conversely, some harmful yet legal content, such as animal harm, eating disorder, dangerous behaviour, may fall outside the protection scope. Instead of focusing solely on age verification as a default measure, the emphasis should be on empowering children to navigate online spaces, building resilience, and fostering connections with supportive figures, including parents, guardians, and educators. This approach ensures a more balanced and nuanced approach to children's online experiences, acknowledging the complexities of content appropriateness in a diverse and evolving digital landscape.

> **Onno Hansen-Staszyński**: "*Children hate seeing animal suffering, but this is currently not illegal for children to look at. We need to know more about children's sensitivities. Scientists, children and regulators should hence cooperate to define what is harmful.*"

3.3.3. Hindrance to Children's Development

Age assurance systems encounter significant challenges in accommodating the evolving capacities of children due to their potential lack of adaptability to the diverse age groups of children. Setting a strict age threshold, like 18 or 16, to restrict access to certain services may overlook the individual needs of children and hinder the construction of their autonomy by preventing them from learning and gradually developing online skills. Instead of abruptly granting access to new services at a specific age, a more effective approach involves providing supportive tools for children to build resilience and navigate online services safely. Relying on the support of parents, legal guardians, and educators becomes crucial in raising awareness and educating children for a secure and informed use of online technologies. This gradual learning process allows children to recognize and manage risks and build their resilience to harmful content. Balancing protection with the empowerment of children is, therefore, essential for creating a safer and more supportive digital environment.

> **Tony Allen (Age Check Certification Scheme)**: *"Children need to be able to gain their own understanding of risk, and that is true in a digital environment as it is in a physical environment. So if you wrap the Internet in cotton wool and make it too safe for children, they don't build the skills and the resilience they need to be able to be adults on the Internet. You have to expose children to proportionate risk to enable them to learn.*"

3.4. Exacerbating Structural Discrimination

3.4.1. Exclusion and Marginalisation

Age assurance systems, while designed to ensure the protection of users, can inadvertently lead to discrimination, posing significant challenges to the respect of the principles of equality and non-discrimination (art. 1 UDHR; art. 14 ECHR; art; 22 CFREU; and art. 2 UNCRC). For example, the reliance of age verification methods on official identity documents leads to the exclusion of individuals who, for various reasons, lack access to or possession of these credentials [40].

Similarly, some age assurance systems rely on digital identities, such as electronic identity card issues by government (eIDs) or tokens issued by trusted authenticators on the basis of official documents. Nevertheless, these technologies are unevenly deployed across European Member States. Residents of European countries where these systems are not available may, hence, be discriminated against if the access to an online service is strictly conditioned to age verification via those systems. Another issue is that, even in countries where digital identities are available, these currently do not concern children. Finally, the wide deployment of these technologies relies on people's ability to navigate through these systems. This can be challenging for people who lack digital literacy or do not have access to sufficiently advanced digital equipment.

Age verification can, hence, affect vulnerable groups, thereby reinforcing societal disparities. This underscores the need for careful consideration in deploying age assurance measures to ensure that they do not inadvertently marginalise certain persons.

3.4.2. Biases and Inaccuracy

The potential bias and inaccuracy inherent in age estimation systems present significant concerns, as they have the propensity to foster discrimination

Facial age estimation are often inaccurate, as they carry the potential for bias, including higher accuracy rates for males than females or lighter skinned people compared to those with darker skin [31]. Closing this gap may take time and increased variety within AI training sets. This requires further data collection from minorities and sometimes marginalised, potentially putting them at higher risk of profiling.

> **Han Hye Jung (Human Rights Watch)**: *"There is no single or easy solution to eliminate discriminatory bias in AI systems. For example, enhancing the diversity and inclusivity of the training dataset - ensuring representation of ages, genders, ethnicities, disabilities, or atypical facial traits – might raise ethical concerns, because the incorporation of people from marginalised communities may inadvertently expose them to higher risks of profiling."*

Moreover, facial age estimation tools often have a margin of error of several years. This inaccuracy can lead to discriminatory outcomes, such as allowing adults into child-only spaces or locking out individuals who are supposed to have access.

> **Joris Duguépéroux (PEReN)**: "*Facial age estimation tools also have the problem of false negatives, meaning people who are adults but are still prevented from using the service because the system have a five year buffer, meaning that if it detect that you are 18 then you will not be granted access. You need to be detected as 23 years old to be able to access the website. So a significant part of the population will be prevented from accessing it.*"

This inaccuracy can lead to discriminatory outcomes, such as allowing adults into child-only spaces or locking out individuals who are supposed to have access.

Similarly, the reliance on statistical models and algorithmic approaches for age estimation can also introduce bias based on the demographic data used in their training. If these models are predominantly trained on data from specific populations, they may not accurately represent the diversity of global demographics.

Finally, task-based methods rely on stereotypes regarding the capabilities of individuals at specific ages. This approach inherently assumes a standard set of skills or tasks associated with certain age groups, perpetuating preconceived notions that may not align with the diverse abilities and experiences of individuals [40]. This can lead to exclusion, particularly for individuals with disabilities or who are neurodivergent, as they may not perform the task as expected.

> **An anonymous lawyer**: "*Children with disabilities or developmental problems may suddenly get put into a group of children much younger than them because they seem to be exhibiting younger age. Besides the potential for discrimination, it is also a categorization of people in the society*."

3.4.3. Feasibility Challenges

Some emerging age assurance technologies, such as digital identities and digital wallets, hold promise from a privacy perspective. However, their adoption encounters notable challenges. Beyond potential technical issues, the absence of digital identities in specific EU Member States, coupled with the current lack of a legal framework at the EU level, prevent its immediate deployment across the European Union.

> **Onno Hansen-Staszyński**: "*The deployment timeline of decentralised identities solutions is minimum 10 to 15 years*."

Moreover, the social acceptance of these technologies may be complicated in specific situations. For example, people may refuse to use a digital identity linked to a governmental tool to access a pornographic website.

> **Joris Duguépéroux (PéREN)**: "*We do not know how people will react if digital identities become the norm. Maybe it will be really hard... there will always be suspicions that the government is trying to know what users are doing.*"

Finally, the high cost associated with their implementation and the difficulties to develop associated economic models may hamper its wide adoption [13].

> **Tony Allen (Age Check Certification Scheme):** *"The proposals for the EU Digital Identity wallets (the EUDI) have a fundamental flaw which is that it has no commercial model underpinning it. It is based on the premise that states will run it and offer it for free. So effectively it's a taxpayer funded model. In my experience that never works or is not sustainable."*

3.5. Failing at Protecting Children Online

3.5.1. Circumvention

It is essential to recognize that all age assurance measures, regardless of their robustness, can be circumvented to varying extents [40]. Age declaration has already been criticised for its lack of reliability, as users may declare a false age without any further check. Age estimation can also be circumvented, for example, using cosmetics and prosthetics to deceive AI facial age estimation or mimicking children's behaviour to deceive AI model analysis. Even age verification based on official documents may eventually be circumvented. For example, by using someone's else document or by altering the document [40], which could lead children who attempt to bypass the age verification measure to commit crime (i.e., identity theft/impersonation or document falsification) [1]. Ultimately, any age assurance measure can be bypassed by utilising a VPN to place the user's IP address in a country where age assurance is not obligatory [20]. Mandating age verification may, as a result, encourage users to relocate to less restrictive jurisdictions that may not guarantee the same level of protection, thereby exposing users, especially children, to heightened risks. Consequently, age assurance measures cannot be perceived as a foolproof solution for children's online protection.

> **Han Hye Jung (Human Rights Watch):** "*Many products and tools that exist today are so inaccurate so that the harms they would cause as a result of their errors would greatly outweigh their claimed benefits.*"

3.5.2. False Sense of Security

As emphasised by EDRi, age assurance measures carry the risk of fostering a deceptive sense of security, where users may wrongly assume that the verified age claimed by an individual is accurate [40]. Although, as all age assurance methods can eventually be bypassed, spaces designated as exclusively for children may potentially harbour malicious actors. For example, relying on parental assistance for age assurance (e.g., via vouching), can introduce the risk of parents utilising their child's account for abusive purposes, such as the excessive surveillance

of their child or the online solicitation of other children. Conversely, the introduction of age assurance measures may also prompt predators to migrate towards less secure services, making detection more challenging.

3.5.3. Absence of Positive Impact

While the intent behind age assurance requirements is to safeguard children online by mitigating their exposure to potentially harmful content and services, there is currently insufficient evidence supporting the capacity of these measures in enhancing children's safety or well-being on the internet or in reducing the risks of online child sexual abuse [31,40].

Given the privacy concerns linked to age assurance technologies and their potential impact on users' fundamental rights, it is essential to explore whether alternative measures could achieve the desired objective in a more secure manner [24]. Approaches such as implementing parental controls, establishing robust reporting systems, refining moderation practices, employing sophisticated recommendation systems, using filtering or warning tools to avoid exposure to harmful content, incorporating easily accessible panic buttons, establishing robust reporting systems for flagging problematic content, and adopting age-appropriate designs prioritising privacy and default safety features may prove to be not only safer but potentially more effective than relying solely on age assurance [31]. Nevertheless, further research and testing are imperative to ascertain the effectiveness and appropriateness of these alternatives. Finally, the importance of education and awareness raising for parents and carers, educators, front-line workers, and children and young people themselves should also be emphasised.

> **Duncan McCann (5Rights Foundation)**: "*We always think about a technological fix that is going to magically fix things up when actually technology, by itself, is not, and cannot, keep children safe. It will be a combination, that must include, society, parents, teachers, friends, etc. playing together.*"
>
> **Onno Hansen-Staszyński**: "*I'm very disappointed by our politicians and policymakers who act as if everything is just a technical solution, but it's not. I think the problem is that most politicians don't understand technology at all, they were not trained for it. So rather than digging deep into the technology and then understanding the consequences that technology decisions might have, they rather just take it as the endpoint.*"
>
> **Han Hye Jung (Human Rights Watch)**: "*Given that many existing methods of age verification risk violating children's rights or other users' rights... It's important to ask the fundamental question: what is it that we want to achieve as a society, and is age verification appropriate for helping us get there? This is a question for policymakers and communities to debate and discuss.*"

4. A RISK-BASED EVALUATION OF AGE ASSURANCE TECHNOLOGIES

This chapter provides an assessment of various age assurance methods in the light of the risks highlighted before in Chapter 3. The evaluation is structured into two parts: the first pertains to the age assurance methods used to collect user's data and establish their age, the second addresses the methods for transmitting the age proof from a third party verifier to the service provider. In both parts, we consider both methods that are already deployed/ deployable and methods currently under development. A table summarising our findings for both parts of the evaluation is available in Table 4.13.

4.1. Evaluation of Age Assurance Methods

As previously mentioned in this study, Chapter 1, age assurance measures are classified into three types: age declaration (cf. Section 4.1.1.), age estimation (cf. Section 4.1.2.), and age verification (cf. Section 4.1.3.). Accordingly, we will adhere to this same structure for our evaluation.

For each age assurance method, we are assessing the likelihood of occurrence of each of the risks listed below. If there is a probability of a specific risk materialising, we also evaluate the severity of its impact on the user. The risks with a potential to occur and to impact users, are listed in Table 4.1. Subsequently, we present a concise summary of this assessment in Table 4.13. at the end of this chapter.

Identified risks. Table 4.1.

User Identification	Data Fraud
Loss of Online Anonymity	Restriction of user's autonomy
Privacy Intrusion	Restriction of user's fundamental rights
Commercial Profiling	Exclusion and Marginalisation
Governmental Profiling	Biases and Inaccuracy
Victim Targeting	Feasibility Challenges
Identity Theft	Circumvention

Among the risks highlighted in the previous Chapter 3, we are not assessing the risks of over-restriction (Section 3.3.2.), hindrance to children's development (Section 3.3.3.), false sense of security (Section 3.5.2.), and absence of positive impact (Section 3.5.3.). This is

because these risks are not contingent on the age assurance methods but rather on the implementation choices made by each service provider concerning the repercussions of the age assurance results on users. These decisions could involve preventing or granting access, restricting access only to a children-only or adult-only version of the services, and restricting or enabling the use of certain features.

Moreover, it is worth noting that the age assurance methods assessed in the first part of our evaluation (cf. Section **4.1.**) may be deployed in various scenarios, impacting the likelihood and severity of the evaluated risks. They might be utilised independently, in conjunction with other age assurance methods, or as part of a broader set of safety measures. Users may also have the option to choose their preferred methods. In situations where the implementation circumstances significantly influence the assessment outcome, a "depends" label is assigned to the likelihood and severity.

Finally, the measures can be implemented either by the provider of the requested online service or by a third party. When a third party conducts the age check, it is crucial to evaluate how the age proof is shared with the service provider. We assess the different methods for sharing age proofs in the second part of Section **4.2.**

4.1.1. Age Declaration

As a reminder, age declaration consists in requesting users to confirm their age by declaring how old they are, but without providing further evidence of their claim. This can be done in different manners, which we detail below. The requested information can vary from a declaration of being above a certain age threshold, to a declaration of the user's exact age, or even to the provision of the user's date of birth. Additionally, providers may request additional steps to "confirm" a user's age, for example, by connecting to the service via an authenticated account, or via an email confirmation. Finally, the age declaration can be done either by the user themselves or by someone else through vouching.

Age declaration methods are clearly the most simple, the least intrusive, and the easiest age assurance methods to implement for providers. According to the EDPB, age declaration may be an appropriate measure to comply with the requirement of article 8 of the GDPR [36]. However, they are also the easiest to circumvent. According to the Ofcom, 32% of UK children aged between 8 and 17 years old have self-declared being 18 or above when registering to a social media [81]. Another study, in Australia, demonstrated that 82% of respondents (i.e., 1500 Australian aged 16) found self-declaration ineffective [88]. For this reason, certain jurisdictions, like France [65,67,68], the UK [119], or several states of the U.S. [85–87,92–94,96,98], explicitly mandate providers of specific services (e.g., pornographic websites [65] or social media [66]) to move away from age declaration methods and adopt age assurance measures that offer a higher level of reliability.

According to our evaluation results, age declaration methods are incontestably less risky for the fundamental rights of both children and adult users. Nevertheless, given their low level

of reliability, they are only suitable for services which present low risks for children or if they are deployed in conjunction with other protective measures, following a holistic approach to online safety [1,19,31,40,55].

4.1.1.1. Self-Declaration

Self-declaration refers to situations where the user declares their age without someone else's intervention.

- **"I'm above 18 years old"**

Probably the easiest, but also less intrusive, way of age assurance is simply to ask users to declare whether they are above or below a certain age threshold. For example, by displaying "yes" and "no" buttons to answer the question. This method only reveals the information necessary to protect children which are below the specified age-threshold and therefore respects the principle of the data minimisation to the greatest extent. Moreover, the provided information is not personal data as it is not possible to directly or indirectly link it to an identifiable person (see art. 4(1) of the GDPR).

Nevertheless, if a user is identified as a child or an adult user, this can impact the user experience, including the potential for enabling some form of profiling (e.g., by adapting the type of commercial communication). Nonetheless, if no other information is collected from children users the risks of profiling remain limited. Conversely, the sole information that a user may be a child may suffice to facilitate potential grooming. Although providers can design measures to mitigate the risk of solicitation of children, if adult and child users are explicitly labelled, it may introduce the risk of child users being targeted by sexual predators. The potential for grooming would, however, be limited if sexual predators lack the means to identify child users or communicate with them.

Lastly, the likelihood of circumvention is quite high, since nothing prevents children users from simply clicking on the button to confirm that they are of sufficient age. This method may, hence, fail in protecting children, which can be problematic depending on the type of provided service and the associated risks. Nevertheless, it still prevent unwanted access to inappropriate content, for example after being unintentionally redirected towards a porn or gambling websites, and raise provide an important signal to children the content of the website is not appropriate for them [31].

Self-declaration of being above/below a certain age threshold. ***Table 4.2.***

RISK	LIKELIHOOD	SEVERITY
Commercial Profiling	low	low
Victim Targeting	depends (on mitigation measures)	very high
Circumvention	very high	depends (on the service provided)

- **"I'm between 25-30 years old"**

Alternatively, providers may ask users about their age-group, or even their actual age. For example, by selecting an age-group (e.g., between 25-30 years old) or by entering their current age (e.g., "I'm 29"). In terms of risks, this method is quite similar to the previous one. The age-group, or even the precise age, are insufficient to identify the user. Nevertheless, the disclosed information is much more precise than a simple declaration of being above a certain age threshold. As a result, the likelihood of the risk of profiling is slightly higher.

Self-declaration of age or age-group. ***Table 4.3.***

RISK	LIKELIHOOD	SEVERITY
Commercial Profiling	low	low
Victim Targeting	depends (on mitigation measures)	very high
Circumvention	very high	depends (on the service provided)

- **"I'm born on the 12/04/1995"**

Providers may also require users to provide their date of birth. However, such information qualifies as personal data protected under the GDPR. It is, indeed, possible to indirectly identify an individual based on their date of birth. This method is thus more intrusive than the previous ones. By collecting the exact date of birth of the user, it processes personal information which is not strictly necessary to achieve the objective of child protection. Consequently, this method is not fully aligned with the respect of the data minimisation principle (art. 5(c) GDPR). Although being limited, the risk of privacy intrusion, therefore, exists.

Dates of birth may also be used for personalised commercial communications, such special birthday offers. The risks associated with commercial profiling are, hence, significantly increased. Additionally, if a sexual predator has knowledge of a child's date of birth, they

could target the child on their birthday, for example, by offering gifts. This situation might increase the likelihood of the child being susceptible to the predator's manipulation.

Regarding the likelihood of circumvention, some consider that providing a date of birth is a "better practice" than simply ticking a checkbox or providing an age because it is less likely to lead to false result [31]. A British study however indicates that individuals who mistrust service providers have a tendency to provide a false date of birth, for example, by keeping the year accurate but changing the day or month [89]. In any case, it is still very easy for a child to indicate a date of birth which is older than its real age.

Self-declaration of date of birth. ***Table 4.4.***

RISK	LIKELIHOOD	SEVERITY
Privacy Intrusion	low	low
Victim Targeting	depends (on mitigation measures)	very high
Commercial Profiling	low-medium	low-medium
Circumvention	very high	depends (on the service provided)

4.1.1.2. Age Declaration Coupled with Email Confirmation

As email addresses may contain information such as name, surname, or company name, there is a possibility of identifying users. This poses a risk of compromising online anonymity and intruding on users' privacy. In fact, the mere collection of an email address already constitutes a privacy intrusion as it potentially allows to correlate the user's activities across various services where the same email is used. Additionally, it establishes a direct communication channel with the user, creating opportunities for direct marketing, but also risks of grooming, scams, and phishing attacks. Furthermore, as the effectiveness of the age assurance process becomes contingent on the good functioning of email services, user's autonomy may be impeded in case of errors or dysfunction. Relying on email addresses may also exclude individuals who either do not possess such an address or choose not to disclose it. Finally, circumventing this age assurance method remains relatively easy for children, as creating an email address requires only basic digital literacy. In summary, while this approach may offer a slightly higher level of reliability compared to simple age self-declarations, it does not furnish conclusive evidence that users are indeed of the age they claim.

Age declaration coupled with email confirmation. ***Table 4.5.***

RISK	LIKELIHOOD	SEVERITY
User Identification	medium	high
Loss of Online Anonymity	medium	high
Privacy Intrusion	medium	high
Commercial Profiling	high	medium-high
Victim Targeting	high	very high
Restriction of User's Autonomy	medium	high
Exclusion and Marginalisation	medium	high
Circumvention	high	depends (on the service provided)

4.1.1.3. Vouching

Vouching allows a trusted entity with an existing relationship with the user to vouch for the user's age. The trusted entity could either be another user (e.g., a parent or carer, including teachers and doctors) or an institution or an organisation (e.g., a bank, a school, a hospital, an employer, a telecommunication provider or an ISP) who previously collected information about the user. The benefits of this method is that it does not require the provision of official identity documents (e.g., government-issued ID cards, passport, birth certificate or driving licence) which may not always be available in all jurisdictions. The Age Verification Providers Association (AVPA) hence promoted vouching as a way to include people who may lack access to official documents or whose age is not accurately assessed by age estimation tools [5].

Nevertheless, the inclusivity of the method depends on the entities which are trusted for the vouching. As acknowledged by the Australian eSafety Commissioner, relationships with institutions such as banks, universities, and hospitals are not universal [31]. In fact, individuals without official documents may find it challenging to rely on such institutional relationships. Similarly, parental vouching creates challenges for children who cannot rely on the support of parents or guardians, either due to their absence or because of a strained relationship.

Although parents expressed their enthusiasm regarding the flexibility and control that vouching mechanism enables [89], children's online freedom may be impeded, in case of excessive parental control over their online activities. This may impact their autonomy and developmental opportunities, especially for older children and teenagers. The lack of autonomy associated with vouching mechanisms also extends to cases where the trusted entity is an institution or organisation as potential delays or refusal in obtaining the vouch as well as the provision of inaccurate information could potentially hinder their access to online services [31].

Vouching also raises privacy concerns. On the one hand, service providers must gather information about an existing relationship between the user and the vouching entity, potentially unveiling sensitive user details with diverse implications. In instances of parental vouching, providers need to establish the parental authority of the voucher over the child user. This may result in the disclosure of identification data, posing a significant risk of profiling for both the parent and the child [1,31]. On the other hand, the vouching entity may acquire insights into the user's online activities while confirming their age. As a result, the social acceptance of vouching varies depending on the nature of the services. It is, indeed, improbable that individuals seeking access to adult content websites, for example, would enlist their bank, doctor, or family to vouch for such purposes.

Nevertheless, vouching could be achieved while implementing the LINC's double-blind approach relying on group signature and zero-knowledge proof (Section **Double-Blind Method**). This method allows the trusted entity to provide a proof-of-age without revealing the user identity, nor their own identity as a trusted entity, while ensuring that the age verification process is robust and reliable. The certified websites for age verification have no information whatsoever on the purpose of this verification and the user's information and browsing habits remain confidential [45].

Lastly, the reliability of age assurance is intricately tied to the credibility of the vouching entities. While institutions like banks, hospitals, or schools are more likely to provide accurate information, social vouching by friends or family may be compromised, with parents potentially aiding children in circumventing age restrictions [89]. As a result, vouching methods are often complemented with further evidence to enhance confidence, such as demonstrating the existence of a "long-term" relationship between the vouching person and the user [123]. This may lead to the provision of additional information, such as both the user's and the entity's identities, consequently increasing the risk of privacy intrusion.

Vouching from trusted entities. ***Table 4.6.***

RISK	LIKELIHOOD	SEVERITY
User Identification	depends (if needed for parental vouching)	high
Loss of Online Anonymity	depends (if needed for parental vouching)	high
Privacy Intrusion	high	depends (on the service provided)
Commercial Profiling	high	high
Governmental Profiling	high	high
Victim Targeting	medium	very high
Restriction of User's Autonomy	very high	high
Restriction of User's fundamental rights	depends (on the service provided)	very high
Exclusion and Marginalisation	medium to high	very high
Circumvention	medium	depends (on the service provided)

4.1.2. Age Estimation

As a reminder, age estimation measures estimate users' age or age-range with a lesser level of accuracy in comparison to document-based age verification. These methods often rely on algorithmic means to analyse user's behavioural and environmental data (Section **AI Profiling**), biometric data (Section **Biomectric Analysis**), or capacity to perform certain tasks (Section **Capacitiy Testing**).

Excluding capacity testing, age estimation relies on the collection of personal data from users, which raises concerns about privacy intrusion. Furthermore, AI systems used for age estimation may have been trained on biased datasets or arbitrary determination criteria, impacting the accuracy of their results and potentially leading to discrimination. Ultimately, the lack of accuracy in the results poses a risk of blocking adults or older children from accessing content or services they are entitled to, while potentially granting adults access to children-only spaces. This classification error may lead children to assume they are in a safe environment, increasing the risk of solicitation.

4.1.2.1. AI Profiling

Profiling involves the processing of user data to analyse and deduce information about them, including their age, without necessitating additional documentation [1,24,31,40]. The efficacy of this method, however, relies on the quality of the profiling dataset. This entails the extensive collection of user data, potentially leading to the disclosure of sensitive information that extends beyond what is essential for age estimation. The data utilised for profiling comprises information users willingly share about themselves but also details that are inferred or automatically collected through their interactions with services (e.g., user's preferences and interests, browser history and cookies, time spent on each webpage, communication patterns, social interactions, cursor movements, or location and time of access) [1]. If these data are aggregated, it may also reveal the user's identity.

The processing of such information raises significant privacy concerns, particularly concerning children, who are not intended to be subjected to commercial profiling, pursuant to recital 71 of the GDPR. Indeed, user profiling rarely serves the sole purpose of age assurance. Its primary objective is rather to personalise the user's experience, optimising their engagement with the service, and facilitating targeted advertising, to maximise the provider's profits. Depending on the invasiveness of the profiling practices and the extent to which the collected data are used to manipulate users towards increased engagement and spending, profiling may interfere with users' fundamental rights, notably the rights to privacy and data protection, freedom of thought, and the children's right to protection against economic exploitation.

Besides commercial purposes, detailed user profiles can also be of interest to third parties, including governmental and law enforcement agencies, for purposes extending beyond mere age assurance. Furthermore, user's details may attract malicious actors seeking to leverage this information to gain a better understanding of their victims' psychology. This may allow them to craft personalised manipulation strategies, increasing the success rate of their attacks. Alternatively, these actors can exploit user behavioural data to mimic their style, with the objective of impersonating them.

In light of the risks associated with profiling, users must be provided with clear and comprehensive information regarding the collection and processing of their data. Without informed consent, engaging in profiling activities would be deemed unlawful under articles 6 and 7 of the GDPR. Additionally, users shall be able to refuse profiling, pursuant to their right to not be subject to automated processing (art. 22 GDPR) [20]. Furthermore, they should be empowered to rectify any inaccuracies in the profiling dataset, in accordance with articles 5(d) and 16 of the GDPR, as profiling datasets may contain errors or biases which could result in unacceptable discrimination. The risk for inaccurate estimation is indeed high as people's behaviour may not always be a reliable indicator of age. Devices and accounts also be shared among family members and friends of various age [24]

Indeed, the determination of the criteria for estimating age are likely to be arbitrary and stereotyped, as the diversity of reasoning and capacities of individuals of various

ages is extremely complex and cannot be easily translated into a technological tool [40]. Consequently, individuals, especially those with disabilities or neurodivergent people, are at a heightened risk of being placed in an age category that does not accurately represent them, thereby hindering their access to parts or the entirety of a service. As a result, using profiling for age assurance creates a substantial risk of discrimination, due to potential inaccurate categorisation of individuals based on the automated analysis of their physical or mental characteristics [40].

Furthermore, for services that are not intended for children, profiling may prove to be an unsuitable method, as it heavily depends on the analysis of data generated from the user's past interactions with the service. This implies that the user has accessed the service before, unless the profiling data were generated from the use of another service, either from the same provider of the restricted-service or from a third party. Nevertheless, sharing profiling data from external sources (e.g., by linking distinct accounts together) creates additional risks, as outlined below in Section **Connection with a Third-Party Account**.

Alternatively, profiling may be used in conjunction with age declaration [31] to verify the level of reliability of the declared age. For instance, Meta monitors public birthday posts on Facebook to compare the ages mentioned in the posts with the age provided by users when signing up to the platform [25]. If the analysis of user behaviour indicates a difference between the two ages, the user may be prompted to go through further age assurance measures. Nevertheless, the extensive collection and analysis of user data, coupled with the potential for discriminatory biases in setting criteria for age determination are likely to render profiling methods disproportionate as a means of age assurance.

Age estimation based on AI profiling. ***Table 4.7.***

RISK	LIKELIHOOD	SEVERITY
User Identification	depends (on datasets)	high
Loss of Online Anonymity	depends (on datasets)	high
Privacy Intrusion	very high	very high
Commercial Profiling	very high	high
Governmental Profiling	high	high
Victim Targeting	high	very high
Identity Theft	medium	very high
Data Fraud	medium	very high
Restriction of User's fundamental rights	depends (on the service provided)	very high
Exclusion and Marginalisation	very high	very high
Biases & Inaccuracy	high	very high

4.1.2.2. Biometric Analysis

Thanks to machine learning models, AI systems can estimate a user's age by analysing their biometric data and identifying similarities with individuals whose age have been verified and recorded into a large training dataset. These biometric data can encompass various physical attributes such as facial features, voice, height, and finger or palm prints [1]. Nonetheless, facial analysis emerges as the most prevalent method for biometric age estimation, as being the most mature of these technologies. demonstrated by the outcomes of the initial pilot of the euConsent project, where 73% of participants exhibited a preference for this method [32]. Facial age estimation's popularity likely arises from its user-friendly nature, offering minimal friction and eliminating the need for official documentation.

Facial analysis for age estimation may, however, raises concerns regarding the protection of individuals' personal data. While facial analysis for age estimation does not possess the capability to identify specific individuals, unlike facial recognition, it does capture images of the user's face. Pursuant to article 9 GDPR, biometric data (including faces) are considered as a special category of personal data for which the processing is only allowed under certain conditions. However, article 9 GDPR only applies to biometric data for the purpose of uniquely identifying a natural person. Furthermore, recital 51 GDPR specifies that the processing of photographs is to be considered as processing of a special category of personal data, under article 9, only when processed through specific technical means allowing the unique identification or authentication of a natural person. Hence, facial analysis for the purpose of age estimation does not fall under the scope of processing of a special category of personal.

> **Tony Allen (Age Check Certification Scheme)**: "*Facial age estimation is done by analysis of facial features but It is not attempting to recognize you or to create a map of your face. It doesn't create enough data to be able to recognize you, so it isn't caught by article 9 GDPR.*"

Nevertheless, faces are still sensitive information, as recognized by the Australian eSafety Commissioner [31]. They intrinsically hold the potential to identify people, as facial features are close to unique (excluding identical offspring). Besides, face can also disclose information which falls within the special category of personal data under article 9 GDPR (e.g., racial or ethnicity origin, or information about health conditions or disabilities affecting facial appearance). Therefore, it is arguable that faces should deserve heightened privacy protections.

> **Alexandra Zeeb-Schwanhäußer (BfDI)**: "*The face of someone is a biometric personal data. So if it is accessed by the facial analysis tool, even for a short period of time with no recording, there would be a personal data processing under the GDPR. However, if the processing of the face does not permit the identification of the person, but only an estimation of the person's age, it does not fall under the article 9 GDPR. But it is still a form of personal data processing which is subject to the provisions of the GDPR.*"

> **An anonymous lawyer**: "*In the UK, ICO had a regulatory sandbox and they concluded that it wasn't biometric identification and thus there was no processing of a special category of personal data under the UK GDPR, because the natural person cannot be identified. However, the person is identifiable at one point in the processing during which there can be security risks, even if the processing happens on the user's device. There is always a moment in time where personal data is being processed*."

If the images of the user's face are not promptly deleted after the age estimation, they might eventually be leaked or used for other purposes, including the identification of the user. To mitigate this risk, the CNIL recommends performing facial analysis locally on the user's device to avoid potential data leak. Although, according to Yoti, running the analysis locally may affect the results accuracy by 8.4% [130].

> **Kostas Flokos (Ageify)**: "*Right now most providers prefer to do the age assurance on their server. However, we can imagine that in the future, with more powerful client side devices, it will be possible to do the age check exclusively on the user's local device*."

If implemented in a protective a way, which involves that the biometrics data are promptly deleted after the age check, these methods may preserve user's anonymity and strongly reduces risks associated with data collection, storage and misuses [31]. It is, however, a matter of trust in the provider's claims on the processing of the collected facial images. Although a provider may declare that the images are not used for identification purpose, that they are fully processed on the user's device rather than being sent to an external server, and that they are promptly deleted once the age check is completed, users lack the ability to verify the veracity of these claims. Hence, in the absence of independent and regular audits, facial analysis systems could potentially hide malicious practices. The CNIL also, hence, emphasises that facial analysis should not be used without an independently verified framework of operating, reliability and performance standards [20].

> **Han Hye Jung (Human Rights Watch)**: "*There does not yet exist peer-reviewed technical research – that is, independent, close scrutiny – that successfully makes the case for the accuracy of proposed age verification methods.*"

Among the potential misuses of biometric data, we could think about the categorisation of people based on their facial characteristics [40]. This could be undertaken by both government or non-state actors to classify people in databases and allow for the targeting of individuals within a certain group. Such classification would particularly affect individuals from racial or ethnic minorities, as well as people with certain health conditions or disabilities, but also children who could be targeted by sexual predators on the basis of their faces. Besides, the collected biometric data could be gathered into datasets to train AI models for various purposes, including malicious ones [1]. The wide deployment of biometric-based systems in the digital landscape as well as the associated social habituation to facial analysis, hence, build the infrastructure for mass surveillance and expose individuals to various types of misuse of their biometric data. For example, malicious actors could set up fake age verification process

to aiming at stealing user's facial images to generate deep fakes, including pornographic ones, use the leaked data to facilitate impersonation, or blackmail to user of a pornographic website to reveal its identity or compromising photos or videos [20].

> **An anonymous lawyer**: "*My big fear is that facial age estimation paves the way for facial recognition technology more broadly and the normalisation of the presentation of faces and biometric data more generally for accessing relatively trivial things.*"
>
> **Han Hye Jung (Human Rights Watch)**: "*As biometric-based systems grow increasingly sophisticated over time, I worry about malicious actors – governments, non-state actors and individuals alike – misusing these systems to violate human rights*."
>
> **Joris Duguépéroux (PEReN)**: "*If tomorrow the access to porn websites is conditioned to facial estimation, it's likely that in a week or maybe in a month, deep fakes will be everywhere and people will have ease to use it and it will be hard to prevent fraud*."

As already mentioned several times, another area of concern which is common to all types of AI-based age estimation systems is the potential for biases in the training dataset leading to inaccuracies in the estimation results. These biases are often due to a lack of representativeness of certain communities in the training datasets. The ICO, indeed, warned that systems based on biometrics, such as hand or facial structure, may perform poorly for people of non-white ethnicity, or for those with medical conditions or disabilities that affect physical appearance [53]. Research literature also found a lack of accuracy for female users as well as certain ethnic groups [62]. As a result, it might be difficult or impossible for certain users to go through the biometric age estimation process or they may be unjustifiably be placed in an age category they do not belong to due to errors in the estimation of their age.

In addition, biometric-based systems necessitate that the user's device is equipped with the relevant sensors to collect biometrics, such as a camera, a fingerprint reader or a microphone. Consequently, some individuals may be excluded from accessing a service which requires biometric if their equipment is not sufficiently modern to be equipped with embedded biometric sensors or whether these are malfunctioning or broken. Moreover, the facial analysis is not suited to people with vision impairment as the method requires users to align their face with an on-screen frame [31]. Similarly, voice assessment requires user to be able to read and speak fluently which can be an issue for people with limited literacy, low language fluency, disability, or simply a different accent [31].

> **Jen Persson (Defend Digital Me)**: "*Facial age estimation is currently failing in terms of accuracy, but even if it does work perfectly and everybody's face becomes their passport, what does it mean for society? We are not properly addressing this societal impact. Face scans are seen as innocuous, unimportant and insignificant for children when they use it in situations that seem to pose no risk to them (e.g., at the school canteen). It is perceived by them in a way that does not see the*

big picture and they're not able, when it comes to these technologies online, to actually provide freely given consent. I think that's a slippery slope that will be detrimental to the balance of power in society and our young people's agency, sense of self, choices and control."

Additionally, facial age estimation is subject to approximations which can lead to wrongly categorised people close to an age threshold. Consequently to be considered as meeting the age requirement a user needs to be estimated 3 to 4 years older than the minimum age threshold. This lead both parents and children in the UK to express doubts about the accuracy of these systems, noting that the appearance of teenagers can vary widely given differences in the age of puberty and development [89].

Finally, biometric age estimation methods can be circumvented with a relative ease [84]. Despite the possibility for facial analysis systems to run a liveness check to make sure the person is real and not a 2D image or bot, children may still ask someone older to scan their face instead of them, or use cosmetics or prosthetics to trick the AI analysis [40].

To conclude, biometric age estimation poses significant risks in case of misuse of biometric information which are inherently sensitive as they hold the potential for user identification, in particular regarding facial data. Nevertheless, these risks may adequately be mitigated if providers of biometric-based age estimation systems implement appropriate measures to ensure the protection of user's data, such as performing the analysis on the user's device to avoid data transfer, as well as deleting the biometric as soon as they become unnecessary. If these safeguards are guaranteed, then biometric-based methods may preserve user's privacy in comparison to other age assurance methods, such as the provision of an official identity document or age estimation based on profiling. Nonetheless, biometric age estimation systems are still immature technologies and can be subject to biases and inaccuracies in their results. Besides leading to potential discrimination, this lack of reliability also prevents biometric age estimation systems from providing a high degree of age assurance. It is, therefore, necessary that service provider who rely on facial age estimation also offer alternative method of age assurance [20].

Age estimation based on biometric analysis. ***Table 4.8.***

RISK	LIKELIHOOD	SEVERITY
User Identification	depends (on the implementation)	high
Loss of Online Anonymity	depends (on the implementation)	high
Privacy Intrusion	depends (on the implementation)	high
Commercial Profiling	depends (on the implementation)	high
Governmental Profiling	depends (on the implementation)	very high
Victim Targeting	depends (on the implementation)	very high
Identity Theft	depends (on the implementation)	very high
Data Fraud	depends (on the implementation)	very high
Restriction of User's Autonomy	high	high
Restriction of User's fundamental rights	depends (on the implementation)	high
Exclusion and Marginalisation	high	very high
Biases & Inaccuracy	high	very high
Circumvention	medium	depends (on the service provided)

4.1.2.3. Capacity Testing

Capacity testing can be used to estimate someone's age by analysing their aptitude and capacity, for example, via reading and language tests, puzzles, maths exercises, or other cognitive assessments [1,31]. However, it cannot determine age with precision but rather indicates whether someone is likely to be above or below a certain age [1].

If this method protects user's privacy as it does require to collect any personal data from users, it, however, involves substantial risk of accessibility challenges and bias [31]. In the

absence of measurable and agreed standards on the relation between age and abilities, capacity testing is likely to be based on stereotypes and assumptions [40]. This could lead to both unreliable results but also discrimination and exclusion. Children of the same age may, indeed, have different skills and abilities [1]. Moreover, individuals with physical or intellectual disabilities, brain injuries, dyslexia, dyscalculia, or neurodivergent conditions may, indeed, have their age inaccurately determined due to their challenges in performing specific tasks, regardless of their actual age [20,31,40].

Finally, it is rather easy for a child to circumvent a capacity test by simply asking an older sibling to do it for them or by searching for solutions on the internet [1,40]. Hence, capacity testing may be adapted for children of very young ages, however, the method's effectiveness significantly decreases the older the child is. Consequently, the method is not suited for instances where a high degree of age assurance is needed.

Age estimation based on capacity testing. ***Table 4.9.***

RISK	LIKELIHOOD	SEVERITY
Exclusion and Marginalisation	high	very high
Biases & Inaccuracy	high	very high
Circumvention	high	depends (on the service provided)

4.1.3. Age Verification

Since age verification implies determining the exact age of an individual with a high level of certainty, it requires the provision of trusted and verifiable data. This could be achieved by providing an official document authenticating the person's identity (e.g., ID card, birth certificate, passport, or driving licence, etc., cf. Section **Official Identity Documents (Hard identifiers)**). Alternatively, governmental and private-issued digital identities are emerging as a mean of electronic identification (eID) allowing users to prove their identity's attributes, including their age, in an electronic format (cf. Section **Electronic Identification (eID) and Digital Identities**). Finally, some service provider rely on proxies of official documentation, such as debit/credit cards, student cards, assuming that the holder of these proxies is an adult (cf. Section **Proxies for Official Documentation**).

None of these methods, however, comply with the principle of data minimisation (art. 5 GDPR), as it reveals much more information than needed to determine someone's age[1,31,40]. The user's identity is, indeed, revealed either to the provider of the service subject to age check or to a third party verifier, allowing for the linkage of the user's online activities to their identity. As a result, age verification measures jeopardise online anonymity and expose user's to the surveillance of their online activities, increasing the risk of misuses of these data for

commercial or policing/political reasons. [40]. Besides, identity data is sensitive information which can be very valuable for malicious actors to commit crimes, such as impersonation or victim targeting. Hence, the collection and retention of this information may expose users to a high risk of identity theft and data fraud[31]. Finally, the loss of online anonymity puts at risk those who rely on it to protect their safety, such as investigation journalists, activists, human rights defenders, whistle-blowers, under-cover agents, sexual workers, or victims of online harassment or abuse) [40].

Furthermore, age verification measures exclude people who lack official documentation, do not possess a credit card or other proxy for official documentation, or do not have records in a trusted database. Age verification requirements could, hence, exacerbate existing social exclusion, especially for individuals from communities that already face high level of structural discrimination (e.g., migrants and asylum seekers, undocumented ethnic minorities, trans and gender diverse people, or other marginalised people - including children in these communities) [1,31,40].

Finally, the systematic reliance on official identity documentation for accessing basic online services dangerously establishes identity control as a norm in everyday life, paving the way for heightened surveillance of individuals' activities. This sense of being constantly observed could potentially deter people from accessing specific information or engaging in certain activities, creating a chilling effect on their behaviour [40]. Therefore, age verification requirements should be implemented only in situations where it is strictly necessary, having regarding to the risks associated with the provided service [17,55].

4.1.3.1. Official Identity Documents (Hard identifiers)

Age verification based on hard identifiers - namely government-issued identity documents, such as ID cards, birth certificates, passports, and driving licences - is a common practice in the off-line environment to access age-restricted products or service, such as tobacco and alcohol products, gambling service, or pornographic content [31]. This information, however, goes well beyond what is necessary to determine someone's age. The intrusion on privacy might cause individuals aware of being under surveillance to refrain from engaging in certain legitimate behaviours, resulting in a chilling effect on their fundamental rights [40]. Extending age verification to the online world also creates substantial risks of data retention and misuse of user's data, as digital technologies allows the verifier to keep this information for an unlimited amount of time and share it with third parties for unknown purposes. Online services may, indeed, stand to benefit commercially from the collection and on-selling of user data [31]. Besides, identity data may, indeed, be of interest to malicious actors who could use or sell these data for fraud or impersonation, especially if the provision of the official document is paired with the collection of user's facial data.

If official identity documents offers a high level of assurance, due to strict proof-of-identity requirements [31], they may still be circumvented, either by using someone else's document or by digitally altering the document's attributes (e.g., date of birth and/or photo) [73]. To prevent fraud, verifiers may ask users to go through a liveness check via a real-time photo or

video of themselves to allow the comparison with the photo on their official document [31]. This comparison check is often performed by an AI system rather than a human, as it requires an individual check for each user which can be extremely burdensome and resource-intensive [40]. However, this automatic processing of facial biometric data poses similar risks than those previously described for facial age estimation (cf. Section **Biomectric Analysis**), especially regarding potential inaccuracies and automated profiling [40]. Moreover, AI-based liveness check goes beyond the mere estimation of age as it implies the recognition of the user's facial traits based on their identity document. Consequently, this processing would be subject to the special rules on biometric data processing for identification purposes laid down in article 9 GDPR [20]. To avoid any risk of misuse, the facial date should be promptly deleted after confirming the user's identity.

Age verification based on official identity documents also creates barriers to inclusion. Indeed, some countries do not have a national identity system or reserve it to people over 16 or 18 years old [40]. Besides, some people may not have official document due to immigration status, language barriers or lack of funds [1]. This would also be the case for victim-survivors of family and domestic violence, and people who have lost documents in natural disasters [31]. Furthermore, birth certificates, passports, or driving licences are not universally accessible [31]. Indeed, they are only issued in specific cases (travelling internationally outside EU or certifying driving abilities). According to data collected by the Australian Passport Office in 2019-20, only 57% of Australians own a passport [11]. Finally, uploading an official identity document may also be challenging for people cannot access relevant digital equipment, as the method requires either a mobile phone with a camera or other means to scan and upload documents [31].

In summary, hard identifiers provide the utmost assurance of a person's age, particularly when complemented with a liveness check. However, it's essential to acknowledge their inherent privacy intrusiveness, which exposes individuals to significant risks of identity theft. Furthermore, relying on official identity documents might inadvertently incentivise users, who attempt to circumvent the measure, to engage in illicit activities, such as using someone else's document or modifying their own document's attributes. Ultimately, age verification measures could always be bypassed by employing a VPN to relocate to a jurisdiction with less stringent regulations, potentially exposing users to additional online risks due to the absence of protective measures in the new location.

Age verification based on official identity documents (hard identifiers). ***Table 4.10.***

RISK	LIKELIHOOD	SEVERITY
User Identification	very high	very high
Loss of Online Anonymity	very high	very high
Privacy Intrusion	very high	very high
Commercial Profiling	high	very high
Governmental Profiling	high	very high
Victim Targeting	high	very high
Identity Theft	high	very high
Data Fraud	high	very high
Restriction of User's Autonomy	very high (if not alternative available)	very high
Restriction of User's fundamental rights	depends (on the service provided)	very high
Exclusion and Marginalisation	very high	very high
Biases & Inaccuracy	depends (if AI-based liveness check)	very high
Circumvention	medium	depends (on the service provided)

4.1.3.2. Electronic Identification (eID) and Digital Identities

Keeping up with the digitalisation of our societal activities, governments in certain European countries developed electronic identification systems (eID), initially, by integrating chips into electronic identity cards, then, by issuing digital identities as digital representations of personal identity. Electronic ID cards allow citizens to scan their ID card via a reader device to provide a certificate presenting only the minimum required information [84]. Similarly, digital identities contain various identity attributes (e.g., name, age, place of birth, citizenship, school and university, address and more) as well as credential (e.g., eID card, e-passport, e-degrees or e-driving licence). Users can store their attribute and credentials in a digital wallet and decide to share their information with the entities of their choice on a granular basis [1,31]. This means that user have control over which attribute they share, with whom and for how long (as permissions can be revoked) [31]. Digital identities may be issued either by governments based on their national database or by private actors after having check official identity documents (e.g., Microsoft Entra Verified ID [77] or MasterCard ID [71]). Digital identity issuers may also provide an associated digital identity wallet, either centralised or

decentralised, or transfer the eID to the user for them to store on their local device. Further details on the specificities of the different digital identity wallets solutions will be provided in the following Section **Age Token**.

Digital identities are, however, not currently available uniformly across Member States of the European Union. This is why the European Commission has proposed, in June 2021, to create a framework for a European digital identity available to all EU citizens [104], as part of the reform of the existing cross-border legal framework for trusted digital identities, the European electronic identification and trust services Regulation (eIDAS proposal) [114]. The EU eID will also be paired with a European digital identity wallet (EUDI Wallet [34]) allowing European citizens to have control over their digital identities' attributes [108]. With this new framework, the European Commission aims to fill the existing digital gap among EU Member states by ensuring that all EU citizens can access both public and private online services via their EU eID all over Europe [109]. The full deployment of an EU-wide eID is, however, not expected before the end of the 2020s [40], while mandatory age verification requirements are already emerging in several Member States. The reliance on eID provision as a mean of age verification would, hence, exclude nationals from countries where eID are not available, fostering existing digital exclusion [40].

> **Kostas Flokos (Ageify)**: "*The problem is the timeline for implementation and deployment of the EUDI wallet as it won't be feasible before 2026-2027, with delays it will probably be more 2030.*"

In theory, digital identities are specifically meant to preserve user's anonymity in situations where the disclosure of their identity is not required, allowing users to reveal a minimised amount of necessary attributes from their digital identity. However, in practice, many services require more information than a mere age attribute (e.g., name, photo, and date of birth, gender, address, etc.) [1]. In this case, age verification via eID could be used as a proxy to collect more data about users, potentially leading to their identification.

Moreover, in the current version of the eIDAS proposal, article 6a(4)(d) states that European digital identity wallets shall provide a mechanism to ensure that the relying party is able to authenticate the user before receiving electronic attestations of attributes [114]. Article 11a of the proposal further specifies that when eIDs and EUDI Wallets are used for authentication, Member States shall ensure unique identification [114]. This means that each eID will be associated with a unique code string which will serve as a unique identifier allowing public and private third parties to identify each user of a digital identity wallet [39]. This would, consequently, negate any privacy benefits of the selective disclosure of attributes [82]. The Commission's proposal, hence, seems to significantly depart from Commissioner Breton's declaration claiming that EUDI Wallets would seamlessly integrate convenience, safety and privacy [39,107]. Conversely, if sharing eID's attributes is conditioned to authentication, the method holds the high potential for governments and private actors to track users online activities with a very high degree of reliability, as the eID is directly link to the user's identity [20,40]. Hence, the authentication of eID's users would critically jeopardise online anonymity and expose people who rely on it for their safety to significant risks (e.g., journalists,

whistle-blowers, people who have experienced online harassment or abuse, sex workers, etc.) [40]. Therefore, it is vital from a privacy perspective that the design of digital identity wallets prevents any central entity from knowing how and where the Wallet App is used, for example, by operating under zero-knowledge and unlinkability paradigm [39]. Privacy-preserving standards already exist for decentralised identity wallets [16,22] and would be far less invasive than the model the Commission is proposing [39]. Consequently, if the provision of eID becomes the norm for daily online activities and no sufficient privacy safeguards are guaranteed, individuals may start to perceive heightened observation of their behaviours, giving rise to a chilling effect on their legitimate activities. [40].

> **Onno Hansen-Staszyński**: "*If a governmental eID tool (e.g., EUDI wallet) is used on a day-to-day basis, for example to access a porn website, it will raise some issues… like the trust in the system and the overall acceptance by the population*."

Another concern in using eIDs as an age verification method is that most of the current national eID frameworks exclude children. Under current eID schemes only adults would, thus, be able to use the method to verify their age. The European Commission, however, encourage Member States to issue eIDs to children to include them in the EU eID framework and allow them to use the European digital identity wallet [105]. Nevertheless, the issuance of eIDs for children raise some concerns as it may lead to the tracking of children's online behaviour. Moreover, if children can freely share their attributes using their digital wallet, without the intervention of their parents or guardians, this may conflict with article 8 of the GDPR. Conversely, if children are dependent on the eID of their parents or guardians, it may expose them to increased risks, in situations from those exercise an excessive control, engage in abusive behaviour, or exploit their surveillance power [40]. Connecting the eIDs of parents with those of their children would also facilitate heightened profiling for both of them [1,31].

> **Kostas Flokos (Ageify)**: "*There are some countries such as the UK where people do not have an ID card nor an eID so for them age verification mechanisms such as face estimation is still very relevant. It's no wonder that most of the age estimation providers reside in the UK because British people don't have an identity document*."

Digital identities hold the highest degree of identity assurance online because they are signed with an official and unique digital signature, which - unlike digital copies of official identity documents - cannot be altered. However, this high reliability makes it an ideal asset for identity theft [1,31,40,126]. The concentration of identity information within an eID stored on governmental or private servers highly incentivises hacks as a successful cyberattack would grant cybercriminals with access to a comprehensive and highly accurate portrait of someone. Digital identity providers should, hence, implement the highest standards of cybersecurity to prevent potential data leaks. However, hackers may also target users, notably via phishing attacks or man-in-the-middle (MITM) attacks. As users often have to scan a QR code to be redirected towards a serve address where they can share their eID and verified signatures with the service provider, attackers may altered such QR code and lead users towards their own server to register the user's eIDs and verified signatures [126].

Doing so, the attacker may steal the user's credential without the user realising and can then use these to impersonate the user without the service provider realising. If eID becomes a widely-spread mean of connection to online services, it would, therefore, only be a matter of time before unauthorised databases with stolen digital identities are created [126]. Control over this data would then be irretrievably lost. A possible mitigation measures would be the obligation for the entity requesting the provision of the eID's attributes to authenticate themselves as a verified and trusted entity to prove that they are not a MITM attacker [126].

> **Onno Hansen-Staszyński**: "*There is a risk of over-sharing, even from data subjects themselves, through the EUDI Wallet or SSI vaults (e.g., in the context of data spaces where people are incentivised to share as much data as possible). However, we are not talking about tracker cookies any more but rather sensitive information that has been validated by a trusted authority. As a result, identity theft could become far more easy. But controllers will say that they are not responsible, that the data subject did it and therefore it is their fault, but they don't do anything to help them make better decisions, on the contrary, they encourage data subjects to provide more data*."

The last blind spot worth mentioning is that this Regulation assumes that everybody in the EU has a smartphone with adequate security to operate the Wallet App safely [39]. However, this assumption may pose challenges, especially for low-income households, where access to compatible devices may be lacking [39,84]. Moreover, as the eID relies on official identity documents initially, it remains inaccessible to undocumented individuals or those who do not want to provide such information [1,40]. Lastly, individuals with lower digital literacy might encounter difficulties in using a digital identity wallet, potentially leading to the inadvertent disclosure of excessive information and making them more susceptible to identity theft [1,39].

> **Kostas Flokos (Ageify)**: "*Actually, even when the EUDI wallet will be available, it is quite probable that not everybody will use it, as it will be optional and not necessarily handy for everyone. So other age verification solutions will remain. It is about finding solutions that are easily accessible by the users that are acceptable by the politicians as well. There will never be a one fit all solution*."

In summary, there is potential for a future digital identity system that authenticates ages in a truly anonymous and permanently untraceable manner, while fully upholding privacy and data protection. However, the realisation of such an infrastructure remains uncertain, even under the eIDAS proposed framework. Furthermore, even if implemented, this system would not resolve the problem of structural exclusion faced by individuals without identity documents, lower income households and people with low digital literacy. [40].

Age Verification based on electronic identification (eID). ***Table 4.11.***

RISK	LIKELIHOOD	SEVERITY
User Identification	depends (on the infrastructure)	very high
Loss of Online Anonymity	depends (on the infrastructure)	very high
Privacy Intrusion	depends (on the infrastructure)	very high
Commercial Profiling	depends (on the infrastructure)	very high
Governmental Profiling	depends (on the infrastructure)	very high
Victim Targeting	very high	very high
Identity Theft	very high	very high
Data Fraud	very high	very high
Restriction of User's Autonomy	very high (if not alternative available)	very high
Restriction of User's fundamental rights	depends (on the service provided)	very high
Exclusion and Marginalisation	very high	very high
Feasibility Challenges	high	/
Circumvention	low	depends (on the provided service)

4.1.3.3. Proxies for Official Documentation

Certain service providers opt for proxies, such as debit or credit cards, student cards, a mobile phone records, or a proof of eligibility [1,6,31,40,84]. Nevertheless, proxies remain highly invasive as they often reveal the user's identity, while being way less reliable than an official identity document. Indeed, proxies do not always divulge the precise age of the holder but rather assume an adult status [1]. This lack of precise age data renders proxies ineffective as an age assurance method. Indeed, the simple assumption that the proxy holder is an adult does not suffice to ensure a high degree of reliability. Indeed, some jurisdictions allow individuals below 18 years old to possess debit or credit cards [84]. Similarly, being 18 years old is not a mandatory condition for university access, making a student card an

insufficient proof of majority. Even in jurisdictions where proxies are intended exclusively for adults, there remains the possibility of a child using someone else's proxy.

Moreover, proxies establish the existence of a connection between their holder and the organisation which issued them. Such information may be highly relevant for profiling purposes. For example, relying on a contract with a telecommunication service provider may reveal the name, date of birth, phone number, physical and email addresses of the proxy holder, which are information which can eventually be used for direct marketing. Additionally, in the case of verification via a payment, the service provider may retain this card information to facilitate the validation of potential future payments. This data retention may expose the user to a risk of data leak and credit data fraud. Besides, the financial institution linked to the debit or credit card may also identify the recipient of the transaction, potentially exposing details about the user's access to specific online services, such as pornographic websites. Consequently, this method allows for a certain degree of privacy intrusion and exposes users to security risks.

Furthermore, proxies fail to address the issue of exclusion, as not all adults have access to debit or credit cards, nor do they possess a student card [20,31,40]. Relying on these proxies may consequently exclude individuals who cannot obtain a credit card due to lower income or favour those with specific educational backgrounds [20,40].

Finally, using credit card payments for age verification may also open avenues for phishing attacks and credit data fraud. Malicious actors could redirect users to a fake website, prompting them to provide credit card credentials to access the service [20]. Hence, it is preferable that the credit card validity check is performed by an independent third party rather than the service to reduce the risk of phishing [20]. Moreover, providers relying on credit cards could launch awareness campaigns and offer alternative methods to users unwilling to share their credentials [20].

Age Verification based on proxies for official documentation. ***Table 4.12.***

RISK	LIKELIHOOD	SEVERITY
User Identification	very high	very high
Loss of Online Anonymity	very high	very high
Privacy Intrusion	very high	very high
Commercial Profiling	high	high
Governmental Profiling	high	high
Victim Targeting	high	very high
Identity Theft	high	very high
Data Fraud	very high	very high
Restriction of User's Autonomy	very high (if not alternative available)	very high
Restriction of User's fundamental rights	depends (on the service provided)	very high
Exclusion and Marginalisation	very high	very high
Biases & Inaccuracy	depends (on the jurisdiction)	high
Circumvention	high	depends (on the service provided)

4.2. Evaluation of Age Proof Transmission Methods

The age assurance methods described before in Section **4.1.** may be conducted either solely by the service provider (Section **4.2.1.**) or with the involvement of a third-party entity acting as a trusted verifier (Section **4.2.2.**). This trusted verifier may be an institution (e.g., a government agency, a hospital, a bank, or a school/university, etc.), a third party service provider (e.g., a very large online platform such as Meta, Apple, Google, or Amazon; a telecommunication or energy provider; or age verification service provider) or a parent or guardian.

When it is a third party who establishes the user's age and issues age proof, the methods for transmitting the age proof to the service provider who requests it may imply different consequences from a privacy perspective. A first concern is whether the service provider is able to identify the user (knowledge of user identity) or whether they only access an age proof without additional user's information. A second concern is whether the service provider gains knowledge about the existence of an establishing relationship with the third party verifier (knowledge of user relationship). Finally, a third is whether the third party verifier can determine who is the service provider who requested the age proof, as it may reveal the

purpose for which the age verification is requested, therefore allowing for a tracking of the user's online activities (knowledge of user behaviour). These three information, especially when they are combined, allow for the surveillance and profiling of the user's activities.

In this section, we examine different methods for sharing age proof and analyse their impact on user profiling. Besides, for each method, we also assess the associated security risks and consider their inclusivity and feasibility. **Table 4.13.** below summarises our findings.

4.2.1. Direct Collection by Service Providers

Service providers who have sufficient resources to develop their own age assurance mechanism may verify their user age themselves, either because they are mandated by law to do so, or because knowing the user's age may help them to better protect children (e.g., by enabling age appropriate designs). Nevertheless, as acknowledged by the CNIL, it is preferable for ensuring a high level of data protection that age verification operation are carried out by an independent third party rather than the service provider themselves [20]. The involvement of a third party, indeed, permits the compartmentalisation of the knowledge regarding the user's identity (knowledge of user identity) and their online activities (knowledge of user behaviour). Depending on the data collected during the age assurance process, the service provider may, indeed, access more information than needed for the purpose of age assurance. As discussed in the first part of our evaluation, the most reliable age assurance methods are also the more invasive. Consequently, services which are subject to the legal obligation of verifying age with a high degree of reliability are very likely to process user's personal data allowing for their identification. Such identification can be highly intrusive, especially for services where the user's activities reveal sensitive information, such as sexual orientation, political opinion or health data. Besides, the linkage of user's activities with their identity exposes them to a significant risk of profiling and other potential misuses of their data.

In terms of security, the integrity of the collected user data depends on the internal measures implemented by each service provider which may greatly vary across providers. In any case, performing age checks directly via the service provider website can increase the risk of phishing, as malicious actors could replicate a service's interface and prompt users to reveal personal information. In that regard the CNIL recommends that verification via credit card payment are performed by an independent third party [20]. Moreover, if facial age estimation is carried out through the interface of a pornographic website using a camera, it could create opportunities for blackmail if compromising photos or videos are recorded by malicious actors [20].

The verification of user age by a service provider itself does not inherently pose a specific risk of social exclusion, as such risks rather depend on the age assurance method used.

Finally, the feasibility to perform the age check directly on the provider's platform depends on their internal resources and capacities.

4.2.2. Third party Age Assurance

To prevent the concentration of user information within the service provider's domain, age verification can be conducted by third-party entities acting as trusted verifiers. Depending on the circumstances, the trusted verifier may be a parent or a guardian (e.g., via a parental vouching mechanism, Section **Vouching**); an institution who has verified identity data about the user (e.g., a government agency, a hospital, a bank, or a school/university); or accredited age verification service provider which can verify or estimate user's age via different methods explained before in Section **4.1.**

To transmit the age proof from the third-party verifier to the service providers, different methods are considered below. The vouching mechanism is not discussed here but was rather explained before (Section **Vouching**) because, unlike the other transmission methods examined, it does not involve the sharing of age proof. Instead, it relies on a simple declaration of a parent or an institution who can prove an existing relationship with the user.

4.2.2.1. Connection with a Third-Party Account

Service providers may also acquire age data from other service providers who previously collected them, for example, by authenticating the user via a third party account (e.g., Google, Apple, Meta, Amazon, Microsoft, X, etc.) However, this method would probably result in heightened privacy intrusion rather than safeguarding user anonymity. Indeed, in the current data-driven economy, online service providers are economically incentivised to collect and share user's personal data to enable the personalisation of their services and maximise user engagement. In practice, researchers found that linking Twitter and Only Fans accounts resulted in the transfer of the user's tweets, account information, and email address. This linkage also empowered the user to post or delete tweets and engage with others on both platforms [1]. Therefore, if the two accounts are linked together, there is a high risk that service providers exchange information about the user, way beyond what is necessary to verify age. Besides, the data transfer also heightens the risk of security breaches as user's data will be available in both provider's servers which offer multiple targets for attackers [31].

Moreover, as the method requires that users have previously checked their age on the third-party platform, it excluded people who do not have a pre-existing account on this platform or choose not to link their account with the service request age verification. Forcing individuals to link to their accounts could prevent them to separate parts of their activities and hinder the exploration of different facets of their identities [31]. Depending on the requested service, this may affect the user's ability to freely express themselves about sensitive topics, to develop new relationships, or to live new experiences. As a result, if such age assurance method is made mandatory, it can significantly impact user's autonomy and lead to a chilling effect on the exercise of their fundamental rights [40].

Finally, the reliability of the age assurance depends on the methods implemented by the third-party. As demonstrated by the 5Rights Foundation, such an age assurance method

can be compromised [1]. Researchers were, indeed, able to register for an Only Fans account (which is restricted to adults) by logging in with a Google account and declaring an age of 13.

4.2.2.2. Age Token

When establishing an age proof, trusted third-party verifiers may either share the data they collected from the user with the service provider or issue an age token which authenticates the user's age or age-range, or eligibility to the service (i.e., being above a certain threshold), without revealing additional user's information, thanks to cryptographic protocols such as zero-knowledge-proof. Zero-knowledge-proof allows a party to prove knowledge of a secret to another party without revealing that secret [42]. Obviously, the first option would negate the whole benefit of relying on a third-party verifier for privacy protection. Conversely, the issuance of an age token would ensure that the service provide remains ignorant about the user identity, unless other identity attributes are disclosed [1,82].

The methods for transmitting the age token from the third-party verifier to service provider may, however, have different privacy and security implications.

- **Age Token Directly Transmitted to Service Providers**

It is possible for the third-party verifier to directly send an age token to the service provider via an API. However this method implies that the verifier knows the identity of the service provider. This information may reveal the purpose of the age verification, allowing the verifier to track user's online activities (knowledge of user behaviour). In an ideal scenario, neither the service provider nor the third-party verifier should know each other. This would avoid the tracking of the user's online activities by the third-party verifier (knowledge of user behaviour) and prevent the service provider from gaining knowledge about an existing relationship between the user and the third party verifier (knowledge of user relationship). This is precisely the approach taken by the LINC, Olivier Blazy and the PEReN, who developed and demonstrated an open-source prototype for a double-blind age verification method which protects user anonymity and privacy [45].

- **Double-Blind Method**

The double-blind method relies on a cryptographic mechanisms (i.e., a combination of group signatures [14,61] and zero-knowledge proofs) to allow third-party verifiers who are certified by a "certifying authority" to anonymously sign a challenge issued by the service provider requiring the age verification [45].

The certifying authority provides specifications (protocol description, formats, etc.) for implementing an age verification system and certifies third parties by adding them to the group of members authorised to issue valid age proofs (via a certificate of their public key valid through the main key of the group). In case where a third party's age verification process is no longer in line with requirements specified by the certifying authority (e.g., because a fake

age proof was issued or no zero-knowledge proof was implement to protect user privacy), the authority adds the public key of that third party to a publicly available revocation list. The third party loses accreditation, and its signatures can be invalidated [45].

When a service provider requests age verification, the process initiates, and a challenge is downloaded to be signed by a certified third party. Each challenge is unique, associated with a required age, and has a limited lifespan. Importantly, the challenge does not reveal the issuer (service provider) [45]. The user must then authenticate with a certified third party of their choice (e.g., a hospital, government services, or an age verification provider) and upload the challenge to verify their age. The certified third party either already knows the user's identity and age or conducts an age verification process if this data is not yet available. The anonymous signature of the challenge can only occur if the user meets the required age to access the age restricted service. If the user has the required age, they can download and share the signed challenge with the service provider to verify its authenticity. The challenge's signature is considered valid only if issued by certified third party and it does not contain information revealing the user's real identity [45].

As a result, the service provider requesting age proof can be certain of the user's age validity without knowing the certifying entity, nor the user's identity or other unnecessary information. Simultaneously, the certified third party is unaware of who issued the challenge and, therefore, does not know which service the user is accessing with the age proof

The question of the transmission of the signed challenge (i.e., the age proof) is, however, crucial, since the double-blindness of the method implies that neither the service provider nor the verifier knows each other. Consequently, the transmission should be carried out an independent and trusted third party can serve as an intermediary between the stakeholders [20]. However, it will be challenging for the latter to make the mere age proof transmission profitable.

> **Joris Duguépéroux (PEReN)**: "*A third-party between the verifier and the porn websites would have a hard time making any money from only transmitting the information*."

The CNIL claims that the trusted third-party transmitting the age proof could take the form of an "attribute management" tool which would allow user to keep a record of their age proof and decide to share with the service providers of their choice (i.e., a digital identity wallet, cf. Section **Digital Identity Wallets**) [20]. In that occasion, the CNIL also mentions the work initiated by the European Commission, notably via its Communication on the new European Strategy for a Better Internet for Kids (BIK+) [105] and the eIDAS proposal [114]. Alternatively, the LINC and the PEReN promote the storage of the age proof in the user's terminal (either in a browser, Section **Age Token at Browser-level**, or in software/app), particularly through automated token exchange like those used in delegation processes (e.g., "OAuth" protocol [80]) or through secured inscription in the user terminal (cf. Section **Age Token at Browser-level**).

While the double-blind approach is very promising from a privacy perspective, its widespread adoption may, however, encounter some challenges, notably due to the complexity of its associated economic models [13].

- **Digital Identity Wallets**

As previously discussed in Section **Electronic Identification (eID) and Digital Identities**, digital identity wallets could enable user to reveal their age attribute in privacy-preserving manner - to the condition that no further data is requested from service providers [1] and that the user is not identified when using its wallet [82]. Several types of wallets may be available to users, each entailing distinct privacy and security considerations.

- **Age Token on Centralised Wallet**

A first option is the storage of the age token on a digital identity wallet offered by a trusted entity, either the third-party verifier itself or another wallet provider (e.g., a governmental organisation or a private company [71]). This wallet will be hosted in the wallet provider's server in a centralised manner. The user's, hence, have to trust the wallet provider not to trace their activities and to keep their credentials safe. As previously discussed in Section **Electronic Identification (eID) and Digital Identities**, eID attributes (incl. age token) are highly valuable asset, notably for identity theft and data fraud [126]. Hence, the centralisation of identity attributes in the hands of a single entity pose significant risk as being targeted by attackers [24,31,40]. Consequently, centralised digital wallet providers shall ensure a high level of security standards, which should be reviewed by independent and qualified third-party auditor [20,55].

A possible preventive measure against fraud could also be the expiration of the tokens' validity after a certain period to avoid that a stolen token would be used for too long. This approach also aligns with token issuers' business models as they currently charge based on token issuance. However, reducing the token validity duration would mean that a new token has to be issued regularly which increases the friction for users.

> **Joris Duguépéroux (PEReN)**: "*The token on the wallet cannot be eternal because, to prevent the attributes to be handed to a child or sold to a black market, the age verification needs to be done in a certain frequency. This question is how frequent that should be.*"
>
> **Kostas Flokos (Ageify)**: "*For the moment, age verification providers try to avoid having a long validity duration for the token for the simple reason that they charge based on the issuance of a token.*"

- **Age Token on Decentralised Wallets**

A second option is to register the age token on a decentralised network (e.g., a distributed ledger technology (DLT), such as a blockchain) [24]. The attributes registered on a DLT are

commonly referred to as decentralised identities (DID) or Self-Sovereign-Identities (SSI). When the age token is generated, it can be encoded into a DLT, using asymmetric encryption, and distributed across all the nodes of the network [76]. The user can then access the token with a pair of public and private keys, which ensure security and privacy [27]. Self-Sovereign Identity (SSI) gives individuals "ownership" and control of their digital identities without relying on a third party, thus avoid the centralisation of their attributes into the hands of a single entity [9]. Users can manage their attributes via a decentralised identity wallet (also called SSI Wallet) and decide whether to grant, refuse, or withdraw access to their digital identity to any entity who requests it [35]. The portability, privacy and security of the SSI are ensured by the adherence to standards and specifications such as those developed by the World Wide Web Consortium (W3C) [128,129]. Relying on SSI wallet, therefore, shifts the user's trust to the technical infrastructure and organisational governance of the decentralised network instead of those of a centralised wallet provider.

Nevertheless, security threats do not necessarily lie in the robustness of the network infrastructure but rather in the possibility of a man-in-the-middle stealing the private key giving access to the SSI wallet [127]. Similarly to the situation previously described concerning eIDs (Section **Electronic Identification (eID) and Digital Identities**), a compromised QR code could redirect the user towards the server of a malicious actor rather than the service provider's one [127]. Without even realising it, the user could, hence, disclose its private key to the wrongdoer who would gain control over their entire SSI wallet, enabling various types of misuses of the user's attributes. In a world where SSI would be exchanged on daily basis, such attack would allow massive fraud opportunities which would most often be unnoticed, as users do not necessarily monitor the activities on their wallet nor service provider ask for a proof that the SSI is shared by the individual associated to it [127]. As even tech-savvy people regularly fall victims to fraud, losing their NFTs and cryptocurrencies, expecting that the whole society, including vulnerable individuals, can effectively protect their digital identities is simply unrealistic [127]

Hence, if SSI becomes the norm, it may exacerbate social inequalities and exclude those with limited access to technology or digital literacy [41,125]. SSI assumes reliable internet connectivity, access to compatible devices, and proficiency in navigating digital systems. Consequently, marginalised populations, including the elderly, individuals in regions with low network coverage, or those with limited technological resources, either by lack of financial means or by a philosophical choice, would face exclusion and reduced access to online services.

> **Sonia Livingstone (London School of Economics)**: "*Probably a third of the society, if not half of it, will actually be unable to use digital identity wallets. Young people, elderly, people with disabilities or mental health conditions, refugees, or simply people with lower digital literacy or who can't afford the equipment. Honestly, we have to ask ourselves who are the beneficiaries of these solutions? Educated white guys? Probably not actual users who share passwords, lose devices and generally don't trust the government or companies*."

- **Age Token on User's Terminal**

Alternatively, a third option is to securely store the age token in the user's terminal (local device). While probably the most privacy-preserving, this method may pose some risks, as the security and integrity of the token would be entirely under the sole responsibility of the user. The method, hence, requires an appropriate level of user awareness to avoid mistakenly deleting the token, losing the device or sharing it with a relative, which can be sources of misuse and circumvention.

- **Age Token at Browser-level**

Finally, it is possible to store the age token on the user's browser, for example, using HTTP cookies [4]. Traditionally, age verification providers used HTTP cookies to share the age proof with the websites browsed by the user, so that when they would not have to do an age check each time they access the website [132].

While this method is convenient for enabling interoperability between multiple service providers and reducing friction for users [4], it also entails privacy and integrity challenges as well as potential circumvention. Indeed, if token issuers have knowledge of the service providers browsed by the user, allowing for profiling of their behaviour (Knowledge of user's behaviour). Besides, age tokens stored as persistent cookies may pose compliance issues with the ePrivacy Directive. The Directive, indeed, requires user's informed consent for the placement of cookies on their terminal equipment and limit the length of time for which a cookie can persist [110]. Finally, users may clear their cookies, thus, deleting the age token; apply incognito or private browsing mode which would prevent the age token to be read by the service provider; or share devices among family members of different ages who can then re-use the token of an older relative [31].

To prevent someone else using the age token, its validity duration may be programmed to expire after a predetermined period, such as after an online session [31]. Some services are, thus, moving away from using browser cookies to rely on session storage instead [7]. Session storage permits to invalid the age token after a series of user interactions on the website or, conversely, a period of inactivity [44]. This method, however, is highly invasive as it relies on the tracking of user behaviour on the online service. Alternatively, other authentication measures, such as on-device biometric recognition or passwords, can also be activated when accessing one's age token, to prevent use by others [31].

4.3. Interim conclusions

The evaluations of both age assurance and age proof transmission methods show that there is currently no single method which simultaneously satisfies sufficient levels of privacy, security, inclusivity and reliability. While age declaration methods limit privacy intrusion, they are not effective in protecting children from accessing services which may be harmful for them. Consequently, where a higher level of age assurance is required, service providers

and age verifiers often turn to either age estimation or age verification methods. On the one hand, age estimation measures avoid the challenge of needing formal legal identity, but create new challenges, such as the systematic and invasive processing of young people's data, contrary to the aims of the Digital Services Act [40]. Besides, given its potential for bias and inaccuracy, age estimation should be avoided as they can misplace users in a wrong age category and be highly discriminatory for a significant part of the population. In the absence of effective and thorough mitigation measures, age estimation methods based on biometric analysis also pose significant risks of misuse of sensitive personal data. On the other hand, age verification methods relying on official identity documents or their digital representations, privacy and security concerns become even more pronounced, as these methods enable user's identification with a high degree of reliability while still allowing for circumvention in case of stolen credentials.

Although the involvement of a trusted third-party verifier issuing a zero-knowledge age token can considerably increase the protection of user's privacy and ensure their online anonymity, especially if it is transmitted to the service provider following a double-blind approach. However, important security and inclusivity concerns remain for all transmission methods, notably regarding the threat of MITM attacks [126,127]. Moreover, despite the European Commission's objective to develop a pan-European framework for digital identities and digital wallets, the wide deployment of such technologies face important obstacles. Robust technical infrastructures are currently not equally available across Member states and the national legislations are fragmented regarding the age threshold for the issuance of digital identity. Finally, There are uncertainties regarding the accessibility of digital identity wallets for European citizens, including vulnerable individuals, and the confidence they are likely to place in these solutions.

Nevertheless, appropriate mitigation measures could reduce some of the above-mentioned risks, enhancing the protection of user's privacy, safeguarding their online anonymity and protecting them from security breaches and misuse of their personal data. In that regard, we align with the requirements set out by EDRi in their position paper which calls for age assurance measures which:

- Permanently prevent any linking of the internet activity or history to the person's identity, or to anonymous or pseudonymous profiles, ensuring that a person cannot be traced (i.e. 'zero knowledge');
- Do not provide any information to the provider other than a yes/no, and not facilitate any access by the provider or by a parent, guardian or other actor;
- Ensure that anonymous use of the internet in general can continue;
- Use tokens instead of storing personal data, and delete personal data processed for the purpose of generating the token immediately afterwards;
- Do not allow any data collected or processed to be used for any other purpose;
- Do not allow the processing of biometric or biometric-based data;

- Refrain from requiring or encouraging all (young) people to have a digital ID, ensuring that people retain a right to analogue;
- Is robust and secure from a cybersecurity perspective;
- Is consensual, and not overly burdensome for those who do not want or do not have the means to verify their identity in this way;
- Is used only where strictly necessary;
- Is mindful of a potential chilling effect, in particular ensuring that access to educational and health (including reproductive health) material is not subject to age verification, which could have a chilling effect on whether or not children feel comfortable accessing this information [40].

These criteria might be articulated within standardisation frameworks for the provision of age assurance solutions as well as guidelines for service providers to identify whether age assurance is needed or if children safety could be achieved within a broader spectrum of protective measures. The next chapter will shortly review existing standardisation and certification frameworks for age assurance systems.

Summary of the risk-based evaluation. ***Table 4.13.***

Method	Reliability	Privacy Preserving	Security & Safety	Inclusivity	Overall Risk Score
Age Declaration					
Self-declared Age Threshold	very low	very high		very high	low
Self-declared Age Range					
Self-declared Date of Birth		medium to high	high		low to medium
Self-declaration with Email Confirmation	low	medium	medium to high	high	medium to high
Vouching		medium to low		medium	
Age Estimation					
AI Profiling	low to medium	very low	medium	low	very high
Biometric Analysis		very low to very high (depending on the implementation)	very low to very high (depending on the implementation)		medium to very high (depending on the implementation)
Capacity Testing	low	high	very high		high
Age Verification					
Official Identity Documents	medium to high	very low	very low	low	very high
eID and Digital Identities	high	low to high (depending on the infrastructure)			low to high (depending on the infrastructure)
Proxies	low	low to very low	low to very low		high to very high

Method		Reliability	Privacy Preserving	Security & Safety	Inclusivity	Overall Risk Score
Age Proof Transmission Methods						
Direct Collection by Service Provider		depends on the age assurance method	very low	low to very low (due to centralisation and potential retention)	depends (on the age assurance method)	very high
Third-Party Age Assurance	Connection with a Third Party Account			very low (due to centralisation, retention and multiplicity of sources)	low (as a third-party account is required)	
	Double-blind method		very high (as group signature and zero knowledge proof are implemented)	depends on the transmission methods	depends (on the age assurance and transmission method)	very low to medium (depending on the transmission method)
	Age Token Directly Transferred to Service Providers		depends on the issuer's ability to identify the user	low to very low (due to centralisation and potential retention)	depends (on the age assurance method)	medium to high
	Age Token on Centralised Wallet		depends on the issuer's ability to identify the user and track the token destination		low (as high digital literacy and modern equipment are needed)	
	Age Token on Decentralised Wallets		very high (when zero knowledge proof is implemented)	medium to low (decentralisation reduce the risk of data leak but MITM attack remain an important threat)		low to medium
	Age Token on User's Terminal		very high	depends on the user own security measures		
	Age Token at Browser-level		depends on the issuer's ability to identify the user and track the token destination	medium (as cookie can be clear and devices shared)	high (works for every with a compute and browser)	medium to high

5. THE ROLE OF STANDARDS AND CERTIFICATION SCHEMES

Among the methods evaluated in the previous chapter, some may be more or less risky depending on the mitigation measures implemented. For example, facial age estimation poses less risks of profiling and identity theft if the facial analysis is performed locally on the user's device without any transfer to an external server, the images are promptly deleted after the age check and no other data are collected, and it is ensure that the automated processing is unable to recognize the user (see Section **Biomectric Analysis**). Similarly, the risks associated with the transmission of an age token based on a digital identity wallet depends on the privacy and security specifications of each wallet solution (see Section **Digital Identity Wallets**). Some may allow for user identification and behavioural tracking while others preserve user privacy to the highest extent, for example adopting a double-blind approach (see Section **Double-Blind Method**). In this context, it is imperative to develop common standards to accurately and reliably evaluate the trustworthiness of age assurance solutions in a reproducible manner. Without thorough auditing, users would lack the means to verify whether the age assurance solution, to which they entrust their personal data, genuinely safeguards that data to the extent claimed by the solution vendor. Additionally, certification schemes may help users and service providers in identifying trustworthy age assurance systems, notably via the creation of a label. Although the effectiveness of such schemes depends on the reliability and integrity of the certification assessment. Therefore, the compliance with the standards shall be assessed by trustworthy, independent, and qualified auditing entities with sufficient technical and organisational resources (including sufficient workforce) [20].

> **Duncan McCann (5Rights Foundation)**: *"Many facial analysis providers claim that no processing of any data is going outside of your computer, that the picture is being taken and analysed all locally and only the result of the test is being sent back to them and then communicated to the third party. When that's true, that's great. But as this technology proliferates, how can you validate it? It is very hard to know. So, it definitely requires this huge element of trust in the provider, which is hard to gain and difficult to sustain in today's digital world given all the data practices that we see going on around us."*

In the United Kingdom, a standardisation and certification framework for age assurance exists since 2018 (see Section **5.1.1.**). Besides international frameworks are currently under development (see Section **5.1.2.** and Section **5.1.3.**). In Germany, the Kommission für Jugendmedienschutz (KJM) has also developed an evaluation scheme for age verification systems (see Section **5.1.4.**). Nevertheless, these standardisation frameworks are not comprehensive as they do not systematically provide requirements for privacy, security, inclusivity and effectiveness. Consequently, we argue that to ensure harmonisation across Member States and guarantee the highest levels of trustworthiness in age assurance

methods, a standardisation and certification framework for age assurance shall be developed at the European level (see Section 5.2.).

5.1. Existing Standardisation and Certification Frameworks

5.1.1. BSI PAS 1296: Online Age Checking & Age Check Certification Scheme

Already in 2018, the British Standards Institution (BSI) released the Publicly Available Specification (PAS) 1296 on "Online age checking. Provision and use of online age check services. Code of Practice." [102]. The PAS provides a code of practice for parties implementing or undertaking age-checking tasks to adopt and demonstrate best practice and compliance in age-checking. Similar to ISO/IEC 27566 (see below), PAS 1296 is not prescribing a specific technology or confidence levels for specific use cases, but "gives recommendations for processes that can be applied when providing and using age check services in order to protect consumers and the online merchant or assist an organisation that wishes to enable enhanced e-safeguarding." As such, the PAS covers security and safety, data protection and privacy, usability and accessibility of age verification systems. Compliance with PAS 1296 can be determined by an independent UK-based accreditation service, the Age Check Certification Scheme (ACCS), which assesses the ability of an age-verification provider or online service on a narrative basis, requiring documentation on their approach to age checking, their data protection and privacy policies, and their quality management. A technical assessment of aspects such as efficacy and equality is not part of this assessment [3].

5.1.2. IEEE Standard 2089-2021 and Draft Standard 2089.1

The Institute of Electrical and Electronics Engineers (IEEE), a US-based professional body for electronic and electrical engineers, approved on the 9 November 2021 a standard aiming at providing a set of processes for digital service when end users are children: The IEEE standard for an Age Appropriate Digital Service Framework based on the 5Rights Principles of Children [100]. The standard does not specifically focus on age assurance but refers to it as a measure to recognise children users and adapt their digital service to their needs (see Section 8 of the standard). The standard emphasises that age assurance mechanisms shall be privacy preserving and proportionate to the risk and nature of the digital service (cf. point (a) of section 8.2) and implemented when necessary (point (2) of section 8.3.) [100]. The standards also provide a definition of the terms "age assurance", "age verification" and "age estimation" (section 3.1) [100]. The standard does not provide further specification regarding age assurance mechanisms.

In September 2021, a draft for a new IEEE standard 2089.1 for Online Age Verification was submitted for approval [50]. This working draft is entirely dedicated to age assurance, providing more detail on the roles and responsibilities of key actors in the age assurance process (section 6), determining the need for age verification (section 7), selecting the method

of age verification, and finally (section 8), establishing standard levels of age assurance based on the level of reliability of the age proof (sections 9 and 10), and determining methods to share the age proof (section 11). The draft standard also considers methods to protect the user privacy and ensure secure operations (sections 12 and 13). The new IEEE standard requires age verification providers to document how age verification attempts are recorded to confirm it is not possible for the platform or service requesting the verification of a user to identify the user, and it is not possible for the provider to record which requesting parties enquired about which of its users. Section 13 also requires the respect of the principle of data minimisation, data security to industry standards, user control over their personal identifier information (PII) and evidence that the system is not vulnerable to penetration [50]. The draft standard, however, does not consider the inclusivity and effectiveness aspects of the age assurance systems. As of February 2024, the submitted draft is not approved yet [51].

5.1.3. ISO/IEC 27566: Age assurance systems

ISO/IEC 27566 is a multi-part standard on "Information technology, cybersecurity and privacy protection – Age assurance systems" that is being developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) [60]. ISO/IEC 27566 is part of the ISO/IEC 27000-series of standards, which provides best practice recommendations on the management of information risks through information security controls within the context of an overall Information security management system [118]. The draft standard on age assurance systems aims at being technology neutral but rather defines levels of confidence in age assurance, ranging from "zero" over "standard" to "strict," where either self-declaration, at least one age assurance component with standard evaluation assurance levels, or multiple such components are involved. The standard further specifies the roles, responsibilities and procedures of key actors in the age assurance process, provides guidance around countermeasures such as anti-spoofing techniques, and lays out data protection, privacy and security requirements for age assurance processes. Specific age assurance thresholds for confidence levels or technologies suitable for specific use cases are not recommended. The standard does, however, define guidance on benchmarks and benchmark analysis of age verification systems with criteria, e.g., for age assurance efficacy and age assurance equality.

On the 27 October 2023, the draft standard ISO/IEC 27566 was deleted [57] and replaced by two new draft standards namely "ISO/IEC WD 27566-1 Age assurance systems. Part 1: Information security, cybersecurity and privacy protection. Age assurance systems Framework. Part 1: Framework" [59] and "ISO/IEC WD 27566-2 Age assurance systems. Part 2: Benchmarks for benchmarking analysis" [58].

5.1.4. Kommission für Jugendmedienschutz in Germany

The German Kommission für Jugendmedienschutz (KJM) has developed an evaluation scheme for age verification systems (latest release in 2022, [63]) and evaluates concepts for complete solutions as well as partial solutions for age verification in closed user groups. The evaluation of modules aims to simplifies the implementation of age verification in practice:

providers can combine positively evaluated modules to develop complete solutions which then fulfil the requirements of the German "Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien" (JMStV) and the KJM. Modules can, for example, only include procedures for identification or authentication or other essential components of an age verification system.

For one-off uses of age-restricted services, the evaluation guide requires an age check, which is carried out again immediately before each use of the system or before each access to a closed user group, e.g., through the use of age confirmation via an eID function. In addition, procedures can be employed that are suitable to determine the age of majority of a person with a high degree of probability, if these procedures are used for every use of the service.

The reliable age verification for repeated-use services requires two steps: a one-time identification and an authentication of the identified person for each usage process. Following a one-off identification of a user and establishing the age of majority of that user, the system is required to issue unique credentials to authenticate the user for subsequent usages of the service. Closed user groups for adults can only be established by means of a reliable age check, with a prerequisite for age verification being personal contact so as to minimise the risk of forgery and circumvention. The face-to-face part of the identification process can, e.g., be provided by post offices, various sales outlets, mobile phone providers, or banks. Camera-based and biometric systems are considered compliant if these "achieve the degree of reliability of a personal age check."

As the KJM scheme prescribes specific implementation approaches, such as the face-to-face age checks, specific governance to ensure efficacy, equality, and equitable access is needed (cf. [20]). The evaluation scheme does not provide requirements or means to assess these properties. Arguably, face-to-face is inclusive but may not be viable, e.g., putting barriers in place in rural regions where a verifying authority is unavailable or where personal barriers to accessing such an authority exist.

The KJM evaluation scheme is, to the best of our knowledge, the oldest evaluation approach for online age-verification concepts. In early 2024, around 50 complete solutions and many more modules have been evaluated positively under this scheme [64]. In contrast to the internationally more established BSI PAS 1296/ACCS, the KJM does consider security but makes no specific provisions regarding privacy and data protection.

> **Alexandra Zeeb-Schwanhäußer (BfDI)**: *"The BfDI (German Federal Commissioner for Data Protection and Freedom of Information) has not been contacted in advance by the KJM regarding the endorsement of age verification solutions. The BfDI has no information that any of the DPAs at landers level was involved."*

5.2. The Need for a Pan-European Framework

In Member states where age verification systems have been mandated by law, national supervisory authorities, such as data protection authorities and media regulators, are requested to provide guidelines on the appropriate age assurance methods that service providers shall implement.

In France, the Act n° 2023-566 [66] and the SREN Proposal [68] both require the Media regulator (the Arcom) to adopt a repository as a standard of reference for the technical requirements of age verification systems. This repository shall determine the minimum technical requirements for age verification systems regarding their reliability and the respect of users' privacy. It shall be established after consulting the opinion of the CNIL and be updated, under the same conditions, each time it is required [68]. In theory, the Arcom will have a period of two months after the enactment of the SREN Proposal to issue its repository [68]. Once published, providers of services subject to age verification will have a period of three months to implement age verification systems complying with the repository [68]. Besides, the Arcom can also require providers to conduct audits by an independent and experienced entity to ensure that their implemented age verification systems comply with the repository [68]. Providers of age assurance solutions who make their solution available on the French market will, hence, have to comply with the Arcom's requirements. It is, however, uncertain - and probably unlikely - that these requirements would follow the same evaluation criteria as those of the KMJ's in its evaluation of age verification modules (see section above).

Consequently, to avoid regulatory fragmentation and ensure the free movement of age assurance solutions within the internal market, the European Union should develop a pan-European standardisation and certification framework. This would be to ensure that among the - yet imperfect - age assurance solutions currently available the highest possible levels of privacy, security, inclusivity and effectiveness are achieved.

Under the new European strategy for a Better Internet for Kids [106], the European Commission has already committed to issuing a standardisation request for a European standard on online age assurance / age verification [105]. The Commission further mentions that this standardisation framework would be developed in the context of the eID proposal, as from 2023 [105]. Although, in February 2024, no draft for a European standardisation scheme has yet emerged.

Meanwhile, in the context of the euConsent project, Age Check Certification Scheme (ACCS) developed three standards (i.e. "certification requirements") within the eIDAS framework and the ETSI standardisation template [33]. These standards encompass age verification [4], parental consent [2], and the trusted certification process for both [4]. It is possible that these standards serve as a basis for the development of a pan-European framework for age assurance. The certification requirements for age verification encompasses some elements of privacy and security. Nevertheless, the inclusivity of the age verification system is not considered.

5.3. Challenges and Critics

In Australia, the eSafety Commissioner carried out a comprehensive research on age assurance methods and engage in a large consultation with various stakeholders over a 12-to-18-month period [31]. When asked about the role of standardisation and certification schemes, the consulted stakeholders agreed that international standards can play an important role in setting baseline requirements, promoting user trust, and facilitating interoperability [31]. Nevertheless, stakeholders also express important concerns, notably regarding perceived or actual conflicts of interest among participants in the standards-making process who may have business interests in the adoption of particular safety technologies [31]. Stakeholders urged inclusive, multi-disciplinary input and a technology-neutral approach which could be applied to a wide variety of existing and emerging technologies [31]. Among the stakeholders interviewed in the context of the present study, some share these views.

> **An anonymous lawyer**: "*Until an independent conformity body is duly established, it is hard to trust private commercial solutions, because the data collection is quite valuable for them.*"
>
> **Duncan McCann (5Rights Foundation)**: "*We need those standards not to be audited by private companies so that we get into another financial auditor situation where it's an old boys club where we order each other and it's all fine. Not only do we need robust standards, we, ideally, need an independent public but yet technical audit function.*"
>
> **Jen Persson (Defend Digital Me)**: "*If we're not careful, child rights impact assessment could be used as a shorthand… I think the problem with impact assessments is that they are only mandated to be carried out within the organisation by the organisation carrying out the practice. Minorities' risks may not be well represented, if at all, in risk assessments. The real risk is that impact assessment becomes only a checkbox exercise to say we have done it. We've considered what we think the risks are, but if the risks are for those users who look like the person carrying out the risk assessment, more than likely they'll miss potential risks and harms which exist for other communities. I think more attention needs to be paid on how risk assessments are carried out and by whom.*"

CONCLUSION

It is undeniable that the protection of minors in the online environment is of paramount necessity in the light of the current risks that online services pose for children's safety and well-being. The recent regulatory initiatives directed at preventing children access to harmful content and services online, therefore, pursue a legitimate objective. Nevertheless, the systematic reliance on age verification as a bullet-proof solution for child protection is both illusive and dangerous.

Our report demonstrated that none of the currently available age assurance methods cumulatively satisfy to a sufficient level the necessary requirements of privacy, security, inclusivity and reliability. All methods of age estimation have proven to be both discriminatory and unreliable, while profiling and biometric-based methods intrude user's privacy enabling various types of misuses of sensitive personal data. While appropriate mitigation measures could partially reduce the risks associated with biometric processing, the current lack of standardisation and certification framework at the EU level expose individuals (both children and adults) to unacceptable risks of commercial and governmental profiling, identity theft and victim targeting. Age verification methods, whether relying on official identity documents or eID, further intensify these privacy and security concerns due to the reliable identification they offer. This identification is however incomplete in the absence of liveness check ensuring that the provided document matches user identity. Such additional verification, however, introduces intolerable intrusion as they most often rely on AI-based facial recognition which are very unlikely to meet the requirements of necessity and proportionality to achieve children's online protection. Additionally, age verification excludes a significant part of the population who do not have access to either an official identity document or an eID.

Zero-knowledge age tokens issued by a trusted third-party, allow a user to prove their age without revealing their identity, thus ensuring anonymity. However, security concerns remain, notably regarding man-in-the-middle attacks [126,127]. Besides, the deployment of a pan-European framework for digital identities and wallets faces challenges which could remain unsolved until the end of the decade. It is also unclear whether the EUDI wallet would actually preserve users' anonymity as article 6a(4)(d) of the eIDAS may allow their identification when sharing attributes [38,39,82]. This could exacerbate risks of profiling, resulting in fear and reluctance towards the solution among potential users. To preserve user's anonymity and prevent the tracking of their online behaviour, a double-blind approach should be implemented throughout the whole transmission of age tokens. Following this approach, service providers requesting the age proof cannot identify neither the user nor the third-party verifier issuing the token. Conversely, the verifier ignores the purpose for which the token is requested as they do not know the identity of the service provider. Nevertheless, the reliance on digital wallets inevitably poses an important risk of social exclusion as the accessibility of these technologies may be challenging for a substantial part of the European

population, including children (particularly those who cannot rely on the support of a parent or caregiver). Furthermore, the lack of digital literacy, especially among vulnerable individuals, may lead to unprecedented instances of identity theft and data fraud if digital identities were required for accessing online services.

As a result, to ensure compliance with the necessity and proportionality principles, age verification should only be implemented when strictly necessary to protect children from harm, having due regards to the risks associated with the provided service. Service providers should, therefore, adopt a risk-based approach and conduct impact assessments to evaluate whether the potential risks stemming from the age assurance method do not outweigh the benefits of preventing children from accessing their services. They should also explore whether alternative measures can be leveraged to achieve the goal of safeguarding children on their platform. For services with a lower level of risks for children but which could benefit from enable age-appropriate designs, a simple age declaration could be sufficient, especially if combined alternative protective measures (e.g., content moderation, appropriate recommendation, absence of targeted advertisement, warning pop-ups, flagging and reporting mechanisms, safety/panic button leading to support tools and assisting team, privacy and safety default settings, or - where appropriate - parental controls) [1,20,24,31,40,55].

When relying on age assurance, users should be informed of the functioning of each age assurance method as well as their associated risks and the mitigation measures implemented by verifiers to reduce these risks. In any case, multiple methods should be available to users to enable them to choose the method they considered the most appropriate having regard to the associated risks. Forcing users into a single age assurance method chosen by the provider may, indeed, violate the requirement for freely given consent under the GDPR.

Regulatory intervention should rather be oriented towards ensuring high levels of privacy, security, inclusivity and reliability in age assurance technologies instead of mandating age verification measures, especially for services which do not present high risks for children's safety and well-being. The adoption of standards and certification frameworks at the European level is crucial to ensure a coherent and trustworthy development of age assurance across Member States. Such frameworks should be paired with thorough auditing of the age assurance technologies performed by trustworthy, independent, and qualified auditing entities with sufficient technical and organisational resources. Additionally, guidelines could be issued by the relevant authorities to support service providers in determining whether their services entails a need for age assurance and, if so, what could be the appropriate measure they could implement to minimise the risk associated with age assurance measures. Guidelines could also highlight the benefits of conceiving age assurance, particularly age declaration, within a broader spectrum of protective measures, providing supportive and awareness raising features rather than restrictive limitations of children's online activities. Finally, regulators and service providers should be reminded that, alongside technical solutions, the involvement of parents, teachers and other educators, social workers, and caregivers remains an important source of support for educating children about digital media and their associated risks.

To conclude, our study reveals a misalignment between the urgency with which governments are pushing for age assurance and the time needed to develop robust, safe and trustworthy age assurance technology. The primary risk lies with the adoption of assurance solutions without adequate protection of individuals' fundamental rights, which could normalise excessive privacy intrusion and heightened risks of data leak and misuses across the online world.

Recommendations

For Regulators

- Regulators - both at European and national levels - should not mandate age verification measures.
- Regulators should allow service providers to rely on age declaration to comply with their legal obligations, in situations which do not present a high risk for children, notably if the age declaration is complemented with other protective measures.
- Accordingly, articles 4 and 6 of the CSAR proposal should be amended to repeal the mandatory requirements for providers of interpersonal communications services and providers of software application stores to implement "age verification and age assessment measures"
- The European legislator should also make clear that the implementation of age assurance measures shall always be aligned with the principles of necessity and proportionality, which mandate to perform an assessment of the risks that age assurance methods may create for the fundamental rights of all users.
- Accordingly, the European legislation should make explicit that the safeguards provided in article 4(2) of the CSAR regarding the mitigation measures implemented by providers of interpersonal communications services and providers of hosting services (including software application stores) apply to "age verification and age assessment measures".
- The European legislator should clarify the meaning of article 6a(4)(d) of the eIDAS and ensure that the European Digital Identity Wallet meets the highest standards of privacy and security requirements by preventing prior electronic identification of the wallet user.
- Regulators, both at European and national levels, should cooperate with the industry to establish pan-European standardisation and certification schemes which ensure, as much as possible, the highest levels of privacy, security, inclusivity, and reliability of the age assurance technologies and age proof transmission methods. Data protection authorities should also be duly consulted.

- Regulators, both at European and national levels, should ensure that regular auditing of the age assurance technologies and age proof transmission methods available on the market are conducted by trustworthy, independent, and qualified entities with sufficient technical and organisational resources.
- Regulators, both at European and national levels, should foster their cooperation to ensure consistent enforcement of European Law in the development and deployment of age assurance technologies across Member States.
- Relevant authorities, preferably at European level to ensure consistency across the Union, should issue guidelines for service providers to determine whether their services pose high risks for children users and whether age assurance may be a necessary and proportionate measure. The guidelines should emphasise potential mitigation measures to reduce the risk associated with the implementation of age assurance and promote the reliance on alternative measures of child protection, when appropriate.
- Regulators, both at European and national levels, should conceive children online protection within a broad spectrum of non-invasive measures, both technical and non-technical, which include the involvement of parents, teachers and other educators, social workers, and caregivers as an important source of children support.

For Providers of Age Assurance Technology

- Ensure the highest levels of privacy, security, inclusivity and reliability in the design and deployment of age assurance technologies.
- Do not collect more information than necessary for establishing user age.
- Rely on privacy-enhancing techniques, such as encryption and zero-knowledge proof, to guarantee user anonymity.
- Ensure that no personal data are retained by the age assurance systems for longer than what is necessary to establish user age.
- Ensure the prompt deletion of unnecessary personal data as soon as they are no longer necessary to establish user age.
- Perform the age assurance processing on user local devices to guarantee a higher degree of privacy and security.
- Prevent any type of misuses of user personal data.
- For age estimation technologies based on biometric data processing, ensure in all situations that no facial recognition is permitted.
- For age estimation technologies based on AI systems, ensure that the training dataset is of the highest quality possible and prevent biases and discrimination in the age estimation results.

- Reflect, develop and implement and promote business models which protect user privacy.

For Third-Party Age Verifiers

- Ensure the highest levels of privacy, security, inclusivity and reliability in the utilisation of age assurance technologies.
- Do not collect more information than necessary for establishing user age.
- Do not collect identity information, unless it is strictly necessary (e.g., to comply with a legal obligation, or due to severity of the risks associated with the provision of the services or certain of their features).
- Ensure that no personal data are retained by the age assurance systems for longer than what is necessary to establish user age.
- Ensure the prompt deletion of unnecessary personal data as soon as they are no longer necessary to establish user age. Do not track user's online behaviour
- Do not track user's online behaviour
- Follow a double-blind approach preventing the identification of the service provider who requests the age proof.
- Prevent any type of misuses of user personal data.
- Provider users with information about the functioning of the age assurance technologies used, the associated risks, and the mitigation measures implemented to minimise these risks.
- Provider users with multiple age assurance options to allow them to choose the methods they consider the most appropriate.
- Reflect, develop and implement and promote business models which protect user privacy.

For Digital Identity Wallet Providers

- Ensure the highest levels of privacy, security, inclusivity and reliability in the transmission of age tokens.
- Do not track user's behaviour through the use of their wallet.
- Do not identify the entities who gain access to the user's wallet.
- Do not reveal the user's identity to the entities who gain access to the user's wallet.
- Make the wallet interfaces easy to navigate and manage, allowing for the highest level of accessibility possible to reduce social exclusion.

- Provide users with information about the functioning of the wallet, the associated risks, and how they can minimise these risks.
- Conduct awareness-raising campaigns on cybersecurity, phishing attacks, man-in-the-middle attacks, identity theft, and data fraud.
- Provide users with accessible and effective support mechanisms, particularly in the event of fraud.
- Reflect, develop and implement and promote business models which protect user privacy.

For Online Service Providers

- Perform regular assessments of the risks associated with their services or certain of their features and their potential impact on children users.
- In cases where their services pose significant risks for children users, assess whether age assurance measures would mitigate these risks.
- Assess the level of assurance needed to ensure children protection, having due regards to the risks associated with the provision of their services or certain of their features.
- Assess the risk associated with each age assurance method considered and evaluate their balance in relation to the risks relating to the provision of their services or certain of their features.
- Assess the impact that the implementation of age assurance requirements may have on users, both children and adults, regarding the exercise of their fundamental rights online.
- Implement mitigation measures to minimise the risks associated with the implementation of age assurance.
- Evaluate whether the protection of children users against the risks associated with the provision of their services or certain of their features can be achieved via alternative protective measures which are less restrictive of the fundamental rights of all users.
- When deciding about the implementation of age assurance requirements, always take the best interest of the child as a primary consideration in the decision-making.
- To achieve all the above recommendations, perform impact assessments, including fundamental rights impact assessments (FRIA) and children rights impact assessments (CRIA) and privacy and data protection impact assessments (PRIA and DPIA). A particular attention should also be paid to the respect of the freedom of expression, right to access information, right to education, freedom

of association, freedom of thought, children's rights to protection against economic exploitation and children's rights to leisure and entertainment.

- Provide users with clear, transparent, concise and easily accessible, and age-appropriate information about the risks related to the provision of their services or certain of their features as well as the functioning of age assurance methods available to users. Emphasise the likelihood and severity of the risks related with each age assurance methods and explained to what extent the implementation of mitigation measures have minimise these risks.
- Provide granular control over the age-related restrictions (if applied to certain features of their services) to accommodate with the evolving capacities of the child, while guaranteeing their safety- and privacy-by design and default.
- Rely on the third-party verifier for the performance of the age assurance, following of double-blind approach to ensure user's anonymity and prevent the establishment of a link between the user and the third-party verifier.
- If the age assurance cannot be performed by a third-party verifier, respect all the recommendations addressed to third-party verifiers as provided above.
- Reflect, develop and implement and promote business models which protect user privacy.

For Research

- Further research on the compliance of the CSAR proposal with children's rights and privacy and data protection laws.
- Further research on the eIDAS proposal with privacy and data protection laws.
- Further research on the impact that mandatory age verification would have on user's fundamental rights, especially those of children.
- Further research on the effectiveness of age assurance measures as a measure to protect children's harm online.
- Further research on the effectiveness of alternative measures; such as content moderation, appropriate recommendation, absence of targeted advertisement, warning pop-ups, flagging and reporting mechanisms, safety/panic button leading to support tools and assisting team, privacy and safety default settings, and parental controls; and evaluate their impact on user's fundamental rights, especially those of children.
- Further research on the feasibility and desirability of digital identity and digital identity wallet as an age proof transmission method.

- Further research on the development of business models which protect user privacy online.
- Engage in discussion with all other relevant stakeholders.

For Society

- Foster the debate around the need for age assurance as a protective measure of children protection.
- Avoid relying on the provision of identity documents as a condition to the participation in the society, in both online and offline realms.
- Provide children with supportive intervention oriented towards their empowerment and the development of their skills, notably regarding digital and media literacy, rather than strict restrictions of their autonomy.

BIBLIOGRAPHY

1. 5RightsFoundation. 2021. But how do they know it is a child? : Age Assurance in the Digital World. Retrieved from https://5rightsfoundation.com/in-action/but-how-do-they-know-it-is-a-child-age-assurance-in-the-digital-world.html

2. Age Check Certification Scheme (ACCS). 2022. euConsent - certification Requirements for Parental Consent. *EuConsent*. Retrieved February 4, 2024 from https://euconsent.eu/download/certification-requirements-for-parental-consent/

3. Age Check Certification Scheme (ACCS). PAS 1296 - Age Check Certification Scheme. Retrieved February 4, 2024 from https://www.accscheme.com/services/age-assurance/pas-1296

4. Age Check Certification Scheme. 2022. euConsent - certification Requirements for Age Verification. *EuConsent*. Retrieved April 28, 2023 from https://euconsent.eu/download/certification-requirements-for-age-verification/

5. Age Verification Providers Association (AVPA). 2023. Age verification methods. Retrieved January 3, 2024 from https://avpassociation.com/avmethods/

6. Age Verification Providers Association (AVPA). Find an AV Provider AVPA. Retrieved January 29, 2024 from https://avpassociation.com/find-an-av-provider/

7. AgeVerify. 2021. Big Change - AgeVerify No Longer Uses Cookies! *AgeVerify*. Retrieved January 30, 2024 from https://ageverify.com/big-change-ageverify-no-longer-uses-cookies/

8. Open AI. ChatGPT. Retrieved May 21, 2023 from https://openai.com/blog/chatgpt

9. Christopher Allen. 2016. The Path to Self-Sovereign Identity. *Life With Alacrity*. Retrieved January 31, 2024 from https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/

10. Article 29 Working Party. 2009. *Opinion 5/2009 on online social networking*. European Commission, Directorate General Justice, Freedom and Security. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf

11. Australian Passport Office. 2018. 2019-20 Passport Facts. *Australian Passport Office*. Retrieved January 26, 2024 from https://www.passports.gov.au/2019-20-passport-facts

12. Luca Bertuzi. 2022. The EU's temptation to break end-to-end encryption. Retrieved December 12, 2023 from https://iapp.org/news/a/the-eus-temptation-to-break-end-to-end-encryption/

13. Martin Biéri. 2023. [Follow-up] - Age verification: The economic argument Linc. Retrieved January 30, 2024 from https://linc.cnil.fr/follow-age-verification-economic-argument

14. Olivier Blazy, Laura Brouilhet, Emmanuel Conchon, and Mathieu Klingler. 2023. Anonymous attribute-based designated verifier signature. *Journal of Ambient Intelligence and Humanized Computing* 14, 10: 1–11. https://doi.org/10.1007/s12652-022-03827-8

15. Cansu Caglar and Abhilash Nair. 2021. EU Member State Legal Framework. Retrieved from https://euconsent.eu/download/eu-member-state-legal-framework/

16. Sarven Capadisli, Amy Guy, and Dmitri Zagidulin. 2022. Did:solid Method Specification. Retrieved January 29, 2024 from https://solid.github.io/did-method-solid/

16bis. Coimisiún na Meán. 2023. Coimisiún na Meán opens public consultation on Ireland's first Online Safety Code. Retrieved February 14, 2024 from https://www.cnam.ie/coimisiun-na-mean-opens-public-consultation-on-irelands-first-online-safety-code/

17. Commission National de l'Information et des Libertés (CNIL). 2021. Recommendation 6: Strengthen the information and rights of children by design. Retrieved from https://www.cnil.fr/en/recommendation-6-strengthen-information-and-rights-children-design

18. Commission Nationale de l'Informatique et des Libertés (CNIL). 2021. CNIL publishes 8 recommendations to enhance the protection of children online. Retrieved from https://www.cnil.fr/en/cnil-publishes-8-recommendations-enhance-protection-children-online

19. Commission Nationale de l'Informatique et des Libertés (CNIL). 2021. Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy | CNIL. Retrieved from https://www.cnil.fr/en/recommendation-7-check-age-child-and-parental-consent-while-respecting-childs-privacy

20. Commission Nationale de l'Informatique et des Libertés (CNIL). 2022. Online age verification: Balancing privacy and the protection of minors. Retrieved from https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

21. eSafety Commissioner. 2023. *Questions, doubts and hopes. Young people's attitudes towards age assurance and age-based restriction of access to online pornography*. Australian Government, Canberra. Retrieved from https://www.esafety.gov.au/sites/default/files/2023-08/Questions-Doubts-and-Hopes.pdf

22. Sam Curren, Tobias Looker, and Oliver Terbu. DIDComm Messaging Specification v2 Editor's Draft. Retrieved January 28, 2024 from https://identity.foundation/didcomm-messaging/spec/

23. Data Protection Commission (DPC). 2023. Irish Data Protection Commission announces 345 million fine of TikTok. *Data Protection Commission*. Retrieved February 2, 2024 from https://www.dataprotection.ie/news-media/irish-dpc-submits-article-60-draft-decision-inquiry-tiktok-0

24. Emma Day. 2021. Digital Age Assurance Tools and Children's Rights Online across the Globe: A Discussion Paper. Retrieved from https://c-fam.org/wp-content/uploads/Digital-Age-Assurance-Tools-and-Childrens-Rights-Online-across-the-Globe.pdf

25. Pavni Diwanji. 2021. How Facebook Knows an App User Is Old Enough. *Meta*. Retrieved January 4, 2024 from https://about.fb.com/news/2021/07/age-verification/

26. Helen Dixon. 1 September 2023. In the matter of TikTok Technology Limited - Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation. Retrieved from https://edpb.europa.eu/system/files/2023-09/final_decision_tiktok_in-21-9-1_-_redacted_8_september_2023.pdf

27. Dock Labs AG. 2024. Self-Sovereign Identity: The Ultimate Guide 2024. Retrieved January 31, 2024 from https://www.dock.io/post/self-sovereign-identity

28. European Data Protection Board (EDPB). 2023. Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR) European Data Protection Board. Retrieved February 3, 2024 from https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22023-dispute-submitted_en

29. Epic Games Inc. 2022. How do I complete the parental consent process? Retrieved from https://www.epicgames.com/help/en-US/epic-games-store-c5719341124379/epic-accounts-c5719350930075/how-do-i-complete-the-parental-consent-process-a12936041250203

30. Epic Games Inc. Verifiable Parental Consent FAQ. *Epic Games*. Retrieved January 29, 2024 from https://www.epicgames.com/site/en-US/parental-consent

31. eSafety Commissioner. 2023. Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography. Retrieved from https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification#roadmap-and-background-report

32. EuConsent. {15 April 2022}. Pilot Execution Report - first large scale euCONSENT pilot. Retrieved from https://euconsent.eu/download/pilot-execution-report-first-large-scale-euconsent-pilot/

33. euConsent. Publications. *EuConsent*. Retrieved February 4, 2024 from https://euconsent.eu/project-deliverables/

34. EUDI Wallet Consortium. 2023. Introducing The EUDI Wallet Consortium. Retrieved January 30, 2024 from https://eudiwalletconsortium.org/

35. European Blockchain Association. SSI Wallets. *European Blockchain Association*. Retrieved January 31, 2024 from https://europeanblockchainassociation.org/ssi-wallets/

36. European Data Protection Board (EDPB). 2020. Guidelines 05/2020 on consent under Regulation 2016/679. Retrieved from https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

37. European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS). 2022. *Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse*. European Data Protection Board (EDPB); European Data Protection Supervisor (EDPS). Retrieved from https://edps.europa.eu/system/files/2022-07/22-07-28_edpb-edps-joint-opinion-csam_en.pdf

38. European Digital Rights (EDRi). 2017. Extending the use of eID to online platforms - risks to privacy? *European Digital Rights (EDRi)*. Retrieved January 28, 2024 from https://edri.org/our-work/eid-online-platforms-risks-privacy/

39. European Digital Rights (EDRi). 2022. Orwell's Wallet: European electronic identity system leads us straight into surveillance capitalism. *European Digital Rights (EDRi)*. Retrieved January 28, 2024 from https://edri.org/our-work/orwells-wallet-european-electronic-identity-system-leads-us-straight-into-surveillance-capitalism/

40. European Digital Rights (EDRi). 2023. Position Paper: Age verification can't 'childproof' the internet. Retrieved from https://edri.org/our-work/policy-paper-age-verification-cant-childproof-the-internet/

41. Alexandra Giannopoulou. 2023. Digital Identity Infrastructures: A Critical Approach of Self-Sovereign Identity. *Digital Society* 2, 2: 18. https://doi.org/10.1007/s44206-023-00049-z

42. Oded Goldreich. 2001. *Foundations of Cryptography: Volume 1: Basic Tools*. Cambridge University Press, Cambridge. https://doi.org/10.1017/CBO9780511546891

43. Google. 2023. Access age-restricted content & features - Google Account Help. Retrieved December 30, 2023 from https://support.google.com/accounts/answer/10071085?sjid=11080147334070030398-AP&visit_id=638236963047512409-1010748356&p=age-verify&rd=1

44. Google. [UA] How a web session is defined in Universal Analytics - Analytics Help. *Google Help Center*. Retrieved January 30, 2024 from https://support.google.com/analytics/answer/2731565\#zippy=\%2Cin-this-article

45. Jérôme Gorin, Martin Biéri, and Côme Brocas. 2022. Demonstration of a privacy-preserving age verification process | LINC. Retrieved from https://linc.cnil.fr/fr/demonstration-privacy-preserving-age-verification-process

46. Guarante per la protezione dei dati personali. 2023. Provvedimento del 2 febbraio 2023 [9852214]. Retrieved February 3, 2024 from https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9852214

47. Guarante per la protezione dei dati personali. 2023. Provvedimento dell'11 aprile 2023 [9874702]. Retrieved February 3, 2024 from https://www.gpdp.it:443/web/guest/home/docweb/-/docweb-display/docweb/9874702

48. Christopher Hutton. 2023. Age verification legislation runs into free-speech legal trouble. *Restoring America*. Retrieved December 29, 2023 from https://www.washingtonexaminer.com/restoring-america/fairness-justice/age-verification-legislation-free-speech-legal-trouble

49. Han Hye Jung. 2022. "How Dare They Peep into My Private Life?" *Human Rights Watch*. Retrieved December 24, 2023 from https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

50. IEEE Standard Association. 2021. *Compliance with IEEE Standards Policies and Procedures*. IEEE Standard Association. Retrieved from https://sagroups.ieee.org/2089-1/wp-content/uploads/sites/451/2021/12/IEEE-P2089.1-Draft-Contribution-8-Dec-2021.pdf

51. IEEE Standard Association. 2021. IEEE P2089.1 Draft Standard for Online Age Verification. *IEEE Standards Association*. Retrieved February 4, 2024 from https://standards.ieee.org

52. Luka Inc. Replika. *replika.com*. Retrieved February 3, 2024 from https://replika.com

53. Information Commissioner Office (ICO). March 2022. Age Assurance: Estimating or Verifying the Age of Service Users. Retrieved March 9, 2023 from https://ico.org.uk/for-organisations/childrens-code-hub/how-to-use-our-guidance-for-standard-one-best-interests-of-the-child/children-s-code-best-interests-framework/age-assurance-estimating-or-verifying-the-age-of-service-users/

54. Information Commissioner Office (ICO). 2020. Age-Appropriate Design Code: A code of practice for online services. Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/

55. Information Commissioner Office (ICO). 2021. Age Assurance for the Children's Code. Retrieved from https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/

56. Irish Data Protection Commission. 2021. Fundamentals for a Child-Oriented Approach to Data Processing. Retrieved from https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf

57. ISO/IEC JTC 1/SC 27. 2023. ISO/IEC WD 27566: Information security, cybersecurity and privacy protection. Age assurance systems framework. *ISO*. Retrieved February 4, 2024 from https://www.iso.org/standard/80399.html

58. ISO/IEC JTC 1/SC 27. 2023. ISO/IEC WD 27566-2: Age assurance systems. Part 2: Benchmarks for benchmarking analysis. Retrieved April 28, 2023 from https://www.iso.org/standard/88147.html

59. ISO/IEC JTC 1/SC 27. 2023. ISO/IEC WD 27566-1. Information security, cybersecurity and privacy protection. Age assurance systems Framework. Part 1: Framework. *ISO*. Retrieved February 4, 2024 from https://www.iso.org/standard/88143.html

60. ISO/IEC JTC1/SC27/WG5. 2021. ISO Working Draft Age Assurance Systems Standard. Retrieved April 28, 2023 from https://euconsent.eu/download/iso-working-draft-age-assurance-systems-standard/

61. Saqib A. Kakvi, Keith M. Martin, Colin Putman, and Elizabeth A. Quaglia. 2023. SoK: Anonymous Credentials. In *Security Standardisation Research*, Felix Günther and Julia Hesse (eds.). Springer Nature Switzerland, Cham, 129–151. https://doi.org/10.1007/978-3-031-30731-7_6

62. Kimmo Kärkkäinen and Jungseock Joo. 2019. FairFace: Face Attribute Dataset for Balanced Race, Gender, and Age. *arXiv.org*. Retrieved December 30, 2023 from https://arxiv.org/abs/1908.04913v1

63. Kommission für Jugendmedienschutz (KJM). 2022. AVS-Raster: Kriterien zur Bewertung von Konzepten für Altersverifikationssysteme als elemente zur Sicherstellung geschlossener Benutzergruppen in Telemedien nach § 4 Abs. 2 S. 2 JMStV. Retrieved from https://www.

kjm-online.de/fileadmin/user_upload/KJM/Aufsicht/Technischer_Jugendmedienschutz/AVS-Raster_ueberarbeitet_gueltig_seit_12.05.2022__004_.pdf

64. Kommission für Jugendmedienschutz (KJM). Altersverifikationssysteme. Retrieved January 30, 2024 from https://www.kjm-online.de/aufsicht/technischer-jugendmedienschutz/unzulaessige-angebote/altersverifikationssysteme

65. L'Assemblée Nationale and Le Sénat. 2020. LOI n 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales (1). Retrieved from https://www.legifrance.gouv.fr/loda/id/JORFTEXT000042176652/2023-11-10/

66. L'Assemblée Nationale and Le Sénat. 2023. LOI n 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne (1). Retrieved from https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047799533

67. Le Premier Ministre. 2021. Décret n 2021-1306 du 7 octobre 2021 relatif aux modalités de mise œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique. Retrieved from https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044173388

68. Le Sénat and L'Assemblée Nationale. 2023. Projet de loi visant à sécuriser et réguler l'espace numérique. Retrieved from https://www.senat.fr/dossier-legislatif/pjl22-593.html

69. Sonia Livingstone and Mariya Stoilova. 2021. *The 4Cs: Classifying Online Risk to Children*. Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI), Hamburg. https://doi.org/10.21241/ssoar.71817

70. Natasha Lomas. 2023. EU commissioner sidesteps MEPs' questions about CSAM proposal microtargeting. *TechCrunch*. Retrieved December 12, 2023 from https://techcrunch.com/2023/10/25/libe-committee-ylva-johansson/

71. MasterCard. Mastercard Innovations Digital ID. Retrieved January 28, 2024 from https://www.mastercard.com.au/en-au/vision/who-we-are/innovations/digital-id.html

72. Duncan McCann, Will Stronge, and Phil Jones. 2021. The Future of Online Advertising. Retrieved from https://www.greens-efa.eu/en/article/document/the-future-of-online-advertising

73. Eric McClure. 2023. How to Make a Fake ID (with Pictures). *wikiHow*. Retrieved January 25, 2024 from https://www.wikihow.com/Make-a-Fake-ID

74. Sebastian Meineck. 2024. Verhütung erst „ab 18": Deutschlands wichtigster Jugendschutz-Filter blockiert Hilfsangebote. *netzpolitik.org*. Retrieved January 22, 2024 from https://netzpolitik.org/2024/verhuetung-erst-ab-18-deutschlands-wichtigster-jugendschutz-filter-blockiert-hilfsangebote/

75. Meta. 2022. Introducing New Ways to Verify Age on Instagram. *Meta*. Retrieved December 30, 2023 from https://about.fb.com/news/2022/06/new-ways-to-verify-age-on-instagram/

76. Microsoft Security. 2022. Decentralized identity and verifiable credentials: Ownership, control, and trust for a digital world. Retrieved from https://query.prod.cms.rt.microsoft.

com/cms/api/am/binary/RE5cxkr?culture=en-us&country=us.

77. Microsoft. 2023. Microsoft Privacy Statement. Retrieved July 17, 2023 from https://privacy.microsoft.com/en-us/privacystatement

78. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. 2021. Code for Children's Rights. Retrieved from https://codevoorkinderrechten.nl/

79. Anna Morgan and Katerina Tassi. 2023. Key points of the DPC's GDPR decision on TikTok and children's data. Retrieved February 2, 2024 from https://iapp.org/news/a/key-points-of-the-irish-dpcs-gdpr-decision-on-tiktok-and-childrens-data/

80. OAuth. OAuth 2.0. Retrieved January 30, 2024 from https://oauth.net/2/

81. Ofcom. 2022. Children's Online User Ages Quantitative Research Study. Retrieved from https://www.ofcom.org.uk/__data/assets/pdf_file/0015/245004/children-user-ages-chart-pack.pdf

82. Alessandro Ortalda, Niko Tsakalakis, and Lina Jasmontaite. 2021. The European Commission Proposal Amending the eIDAS Regulation (EU) No 910/2014: A personal data protection perspective. *Brussels Privacy Hub*. Retrieved from https://brusselsprivacyhub.eu/onewebmedia/Proposal%20to%20amend%20eIDAS.%20A%20personal%20data%20protection%20perspective_BPH_December%202021.pdf

83. Emma Pinedo. 2023. Spain readies age-checking tech to protect children from adult online content. *Reuters*. Retrieved January 28, 2024 from https://www.reuters.com/world/europe/spain-readies-age-checking-tech-protect-children-adult-online-content-2023-12-14/

84. Pôle d'expertise de la régulation numérique (PEReN). 2022. Online underage users detection: Can we reconcile efficiency, convenience and anonymity? Retrieved from https://www.peren.gouv.fr/rapports/2022-06-23%20-%20Eclairage-sur-detection-mineurs_EN.pdf

85. Rep. Eubanks. 2023. An act to regulate pornographic media exposure to children; to provide the legislative intent; to provide definitions; to require commercial entities that provide such content to have age verification systems; to provide liability for those commercial entities that do not provide an age verification; to bring forward sections 97-29-107 and 97-29-109, Mississippi code of 1972, which provide the exemptions and penalties for distribution of obscene materials, for purposes of amendment; and for related purposes., HB1315, State of Mississippi. Retrieved February 3, 2024 from https://billstatus.ls.state.ms.us/documents/2023/html/HB/1300-1399/HB1315IN.htm

86. Rep. Phelps, Tammy, Rep. Landry, Mandie, Rep. Moore, Pat, and Rep. Schlegel, Laurie. 2022. Louisiana House Bill 440LA HB440. Retrieved from https://legiscan.com/LA/bill/HB440/2022

87. Rep. Shaheen. 2023. An act relating to the publication or distribution of sexual material harmful to minors on an internet website; providing a civil penalty., HB 1181, State of Texas. Retrieved February 3, 2024 from https://capitol.texas.gov/BillLookup/History.aspx?LegSess=88R&Bill=HB1181

88. Resolve. 2022. Consolidated Industry Codes of Practice for On-line Class 1 Content

Community Research (Commissioned by Digital Industry Group Inc and Communications Alliance). Retrieved from https://onlinesafety.org.au/wp-content/uploads/2022/10/R220719-DIGI-CA-Project-Class-1-Sep-2022-Survey-Results-PUBLIC-RELEASE.pdf

89. Revealing Reality. 2022. Family attitudes towards age assurance (commissioned by ofcom and ICO). Retrieved from https://revealingreality.co.uk/families-attitudes-towards-age-assurance/

90. Roblox. 2021. Introducing Age Verification. *Roblox Blog*. Retrieved December 30, 2023 from http://https\%253A\%252F\%252Fblog.roblox.com\%252F2021\%252F09\%252Fintroducing-age-verification\%252F

91. Johnny Ryan. 2021. Europe's enforcement paralysis: ICCL's 2021 GDPR report. *Irish Council for Civil Liberties*. Retrieved August 5, 2022 from https://www.iccl.ie/digital-data/2021-gdpr-report/

92. Sen. Blumenthal. 2023. Kids Online Safety Act, s-1409, U.S. Congress, 118th session. Retrieved February 2, 2024 from https://www.congress.gov/bill/118th-congress/senate-bill/1409

93. Sen. Curdy. 2023. An act revising internet laws related to material harmful to minors; providing for liability for the publishing or distribution of material harmful to minors on the internet; providing for reasonable age verification; providing for individual rights of action; providing for attorney fees, court costs, and punitive damages; providing for exceptions; requiring a report by the department of justice for enforcement activity; providing for a fee; providing definitions; and providing a delayed effective date., SB 544, State of Montana. Retrieved February 3, 2024 from https://leg.mt.gov/bills/2023/billhtml/HB0234.htm

94. Sen. Dees and Sen. Petty. 2023. An act to create the social media safety act; to require age verification for use of social media; and to clarify liability for failure to perform age verification for use of social media and illegal retention of data penalty, SB396, State of Arkansas. Retrieved February 3, 2024 from https://www.arkleg.state.ar.us/Bills/Detail

95. Sen. Miville-Dechêne. 2021. Protecting Young Persons from Exposure to Pornography Act, s-210 (44-1), parliament of canada. Retrieved February 3, 2024 from https://www.parl.ca/DocumentViewer/en/44-1/bill/S-210/first-reading

96. Sen. Weiler and Rep. Pulsipher. 2023. Online Pornography Viewing Age Requirements, SB 287, State of Utah. Retrieved from https://le.utah.gov/~2023/bills/static/SB0287.html

97. Sen. Wicks, Sen. Cunningham, and Sen. Petrie-Norris. 2022. The California Age-Appropriate Design Code Act, AB 2273, State of California. Retrieved from https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220AB2273&showamends=false

98. Sen. William. 2023. Harmful materials; civil liability for publishing or distributing to minors on the Internet, SB 1515, State of Virginia. Retrieved February 3, 2024 from https://lis.virginia.gov/cgi-bin/legp604.exe?231+sum+SB1515

99. Furvah Shah. 2021. Facial recognition cameras installed in UK school canteens. *The Independent*. Retrieved December 27, 2023 from https://www.independent.co.uk/news/education/education-news/facial-recognition-uk-school-canteens-b1940109.html

100. Standards Committee of the IEEE Consumer Technology Society. 2021. IEEE Standard 2089-2021 for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children. https://doi.org/10.1109/IEEESTD.2021.9627644

101. Luděk Stavinoha, Apostolis Fotiadis, and Giacomo Zandonini. 2023. "Who Benefits?" Inside the EU's Fight over Scanning for Child Sex Content. *Balkan Insight*. Retrieved December 12, 2023 from https://balkaninsight.com/2023/09/25/who-benefits-inside-the-eus-fight-over-scanning-for-child-sex-content/

102. The British Standard Institution (BSI). 2018. PAS 1296:2018 - Online age checking. Provision and use of online age check services. Code of Practice. Retrieved February 4, 2024 from https://knowledge.bsigroup.com/products/online-age-checking-provision-and-use-of-online-age-check-services-code-of-practice?version=standard

103. The Council of Europe. 1950. *European convention on human rights*. The Council of Europe. Retrieved from https://www.echr.coe.int/documents/d/echr/Convention_ENG

104. The European Commission. 2021. Commission proposes a trusted and secure Digital Identity. *European Commission - European Commission*. Retrieved January 28, 2024 from https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663

105. The European Commission. 2022. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Decade for children and youth: The new European strategy for a better internet for kids (BIK+). Retrieved January 29, 2024 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:212:FIN

106. The European Commission. 2022. New European strategy for a Better Internet for Kids. *European Commission - European Commission*. Retrieved February 4, 2024 from https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_2826

107. The European Commission. 2023. Provisional political agreement EU Digital Identity Wallet. *European Commission - European Commission*. Retrieved January 28, 2024 from https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3556

108. The European Commission. 2023. Q&A: European Digital Identity. *European Commission - European Commission*. Retrieved January 28, 2024 from https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_2664

109. The European Commission. 2023. Final agreement on EU Digital Identity Wallet. *European Commission - European Commission*. Retrieved January 28, 2024 from https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5651

110. The European Parliament and The Council. 2002. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Retrieved March 13, 2023 from http://data.europa.eu/eli/dir/2002/58/2009-12-19/eng

111. The European Parliament and The Council. 2015. Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for

the provision of information in the field of technical regulations and of rules on Information Society services (codification) (Text with EEA relevance). *241*. Retrieved December 21, 2023 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L1535

112. The European Parliament and The Council. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). p. 1–88. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

113. The European Parliament and The Council. 2018. Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (codified version) (Text with EEA relevance)Text with EEA relevance. Retrieved from http://data.europa.eu/eli/dir/2010/13/2018-12-18/eng

114. The European Parliament and The Council. 2021. Proposal for a regulation of the European parliament and of the council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. Retrieved April 27, 2023 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281

115. The European Parliament and The Council. 2022. Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (CSAR). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:209:FIN

116. The European Parliament and The Council. 2022. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/2065/oj

117. The European Parliament, The Council, and The European Commission. 2012. Charter of fundamental rights of the European union. *Official Journal* C 326/395: 17. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

118. The International Organization for Standardization (ISO). 2022. ISO - ISO/IEC 27000 family Information security management. *ISO*. Retrieved February 4, 2024 from https://www.iso.org/standard/iso-iec-27000-family

119. The Parliament of the United Kingdom. 2023. Online Safety Act 2023. Retrieved from https://www.legislation.gov.uk/ukpga/2023/50/enacted

120. The Social Research Centre. 2022. *The 2022 National Online Safety survey – summary report*. Australian Government, Melbourne. Retrieved from https://www.infrastructure.gov.au/sites/default/files/documents/national-online-safety-survey-2022-wcag-accessible-report-25july2022-final.pdf

121. The United Nations. November 1989. Convention on the Rights of the Child. Retrieved from https://www.ohchr.org/sites/default/files/crc.pdf

122. The United Nations. 1948. Universal declaration of human rights. Retrieved from https://www.ohchr.org/en/human-rights/universal-declaration/translations/english

123. UK Government Digital Service. 2020. How to accept a vouch as evidence of someone's identity. *GOV.UK*. Retrieved January 3, 2024 from https://www.gov.uk/government/publications/how-to-accept-a-vouch-as-evidence-of-someones-identity/how-to-accept-a-vouch-as-evidence-of-someones-identity

124. Valerie Verdoodt. 2020. *Children's Rights and Commercial Communication in the Digital Era: Towards an Empowering Regulatory Framework for Commercial Communication*. Intersentia. https://doi.org/10.1017/9781780689418

125. Linda Weigl, Tom Barbereau, Alexander Rieger, and Gilbert Fridgen. 2022. The Social Construction of Self-Sovereign Identity: An Extended Model of Interpretive Flexibility. In *Hawaii International Conference on System Sciences*. https://doi.org/10.24251/HICSS.2022.316

126. Lilith Wittmann. 2021. Mit der ID-Wallet kannst Du alles und jeder sein, außer Du musst Dich ausweisen. *Medium*. Retrieved April 27, 2023 from https://lilithwittmann.medium.com/mit-der-id-wallet-kannst-du-alles-und-jeder-sein-au%C3%9Fer-du-musst-dich-ausweisen-829293739fa0

127. Lilith Wittmann. 2022. Mit dem Personalausweis zum Onlineshopping: Wie selbstbestimmt sind "selbstbestimmte Identitäten"? *Medium*. Retrieved April 27, 2023 from https://lilithwittmann.medium.com/mit-dem-personalausweis-zum-onlineshopping-wie-selbstbestimmt-sind-selbstbestimmte-identit%C3%A4ten-f096a5bdd55a

128. World Wide Web Consortium (W3C{}. 2022. Verifiable Credentials Data Model v1.1. Retrieved January 31, 2024 from https://www.w3.org/TR/vc-data-model/

129. World Wide Web Consortium (W3C{}. 2022. Decentralized Identifiers (DIDs) v1.0. Retrieved January 31, 2024 from https://www.w3.org/TR/did-core/

130. Yoti. 2022. Yoti Age Estimation White Paper. Retrieved from https://www.yoti.com/wp-content/uploads/Yoti-Age-Estimation-White-Paper-May-2022.pdf

131. Yoti. 2023. How OnlyFans became the first UK subscription-based platform to protect children and create age-appropriate experiences Yoti. *Yoti*. Retrieved December 30, 2023 from https://www.yoti.com/wp-content/uploads/Onlyfans_Case-Study_120623.pdf

132. Yoti. Reusable age checks - Yoti developer documentation. Retrieved February 1, 2024 from https://developers.yoti.com/v8.0/age-verification/age-tokens

133. Yubo. 2022. Yubo's new age verification feature helps keep you safe. *Yubo*. Retrieved December 30, 2023 from https://www.yubo.live/blog/yubos-new-age-verification-feature-helps-keep-you-safe

Layout: OKAY WHEN agency

Cover image: Unsplash/Tim Gouw

THE GREENS/EFA in the European Parliament

60 rue Wiertz/Wiertzstraat 60
1047 Brussels, Belgium
www.greens-efa.eu
contactgreens@ep.europa.eu