EDRi

European Digital Rights

Position paper

Online age verification and children's rights

4 October 2023

This paper represents the joint position of 20 civil society organisations: Alternatif Bilisim (Turkey), ApTI (Romania), Bits of Freedom (the Netherlands), CCC (Germany), Defend Digital Me (United Kingdom), Digitalcourage (Germany), Digitale Gesellschaft (Switzerland), Electronic Frontier Foundation (international), EFN (Norway), epicenter.works (Austria), ESWA (Europe), European Digital Rights (Europe), FIPR (United Kingdom), Homo Digitalis (Greece), the Irish Council for Civil Liberties (Ireland), IT-Pol (Denmark), Metamorphosis Foundation (North Macedonia), Politiscope (Croatia), SHARE Foundation (Serbia) and SUPERRR Lab (Germany).

Table of Contents

Published in Brussels, 4 October 2023.

European Digital Rights (EDRi) is sincerely grateful to our members and partners who supported with the research, drafting and review of this paper.

Executive summary

Lawmakers are increasingly turning to age verification as a way to tackle online harms and illegal activities, for example in the draft EU Child Sexual Abuse Regulation. But whilst the EU age verification industry alone is reaching a value of several billion euros, there is a lack of evidence that age verification measures improve the safety of children online.

This study finds that with the exception of age declaration methods, age verification threatens the privacy, data protection and free expression rights of children and adults alike. This can erode democratic freedoms that rely on anonymity online (e.g. journalism), violate children's autonomy, and disempower parents and guardians.

Such measures are also likely to have the most profound negative consequences for children and adults who already face high levels of structural exclusion or discrimination and those with low levels of digital literacy. We find that in particular, document-based age verification and age estimation are unlikely to pass the human rights test of necessity and proportionality.

1. Age declaration:

- Age declaration is the term for measures that ask a person to provide their age:
- This study finds that these methods pose the fewest risks to everyone's rights online, and are already legal in the EU under the GDPR. New guidelines could help implement them;
- However, these measures are also the most likely to be circumvented, so in order to be effective, should be seen as part of a holistic approach including privacy and safety by design, content labelling, parental/guardian trust and oversight, and education.

2. Document-based age verification:

- Sometimes referred to simply as age verification, this means measures that capture information from a formal document (such as a passport scan, an eID or a credit card);
- Whilst in theory, such measures could be done in a way which protects people's data, this study finds that current and foreseeable methods of document-based age verification create high risks of data breaches, pervasive online tracking, a chilling effect on legitimate activities and of exacerbating structural exclusion;
- Such measures should not be mandated. Their case-by-case use should be strictly controlled, safeguarded, and only when strictly necessary (i.e. not on a widespread basis).

3. Age estimation:

- Age estimation refers to measures which predict or estimate people's age, for example based on their interactions or by using AI-based tools to analyse their face;
- Such measures rely on mass data gathering or toxic business practices (e.g. profiling). Frequently this includes the processing of children's sensitive biometric data;
- As such, age estimation measures pose an unacceptable risk and should not be used.

Introduction

Governments around the world are increasingly proposing laws and policies aimed at tackling the risks for children (defined in the *UN Convention on the Rights of the Child* as anyone under 18 years of age) which may arise when they use certain online spaces or take part in certain online activities. **Measures to systematically assess people's age online have been presented by the growing age verification industry as if they were a silver bullet for the risks that children face in the online environment.** Proposals to mandate online age verification have been seen in the US, UK, India, Australia, the EU and more.

This paper is focused on the issue of online age verification and its three main types (document-based verification, estimation and declaration), with particular attention to the EU context and rules in the EU's *General Data Protection Regulation*. This issue is pressing in the EU because the draft *Child Sexual Abuse* (CSA) *Regulation* proposes to mandate forms of age verification for private message services (e.g. WhatsApp, Signal) and app stores operating in the EU, and to strongly incentivise it for all other digital platforms and services, such as social media.[1]

The issue of online age verification is complex. There is a legitimate need to ensure that children can access content that is considered legally appropriate for their age. Some countries have national rules relating to access to specific age-restricted services (e.g. gambling). More broadly, there is an obligation on governments and companies to protect children from abuse, manipulation and exploitation online (all of which can infringe on their dignity, privacy and more).

However, **there is a lack of evidence that the widespread adoption of online age verification systems as a precursor for accessing private messaging, app downloads, or social media will keep children safe**. Currently available measures to undertake age verification come with potentially serious human rights impacts – in particular for the children they are supposed to protect. **One of the aims of this paper is to raise awareness of the fact that age verification measures should not be seen as a straightforward solution to illegal activities such as online child abuse**. An over-focus on implementing age verification systems may obfuscate the societal problems that facilitate or exacerbate online harms in the first place, by framing the issue as a technical one, when in fact it is deeply human. **A more holistic approach, which considers age verification as a spectrum of supportive, rather than restrictive, measures – based in privacy and safety by design - is more likely to be effective and rights-respecting.**

As the United Nations and UNICEF both emphasise, children have rights to freedom of expression and access to information online.[2] Their autonomy and self-development – which can be an important part of the exploration of their identity, for example their sexuality or their democratic participation – rely on being able to freely search and communicate online. With digital tools being a large part of the lives of most young people, and especially in the wake of the COVID-19

1 The proposal by the European Commission refers to 'age verification and age assessment' measures. This would exclude self-declarations (such as entering a date of birth) but permit checks using legal identity documents or predictive (i.e. AI-based) tools.

2 United Nations General Comment 25: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2FC%2FGC%2F25&Lang=en; UNICEF Children's Online Privacy and Freedom of Expression Industry Toolkit: https://sites.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf

pandemic, everything from education to entertainment has become even more digitalised. Any measures that could result in limiting or controlling young people's access to legitimate online services and content should therefore be approached with extreme caution.

There are serious risks for adults and children alike if anonymous access to the internet is made difficult or impossible, as well as risks of digital exclusion for those without access to the right tools or documents. As a society, we have seen little consideration about whether it is even desirable to normalise the need for identity documents to take part in society. On the contrary, EDRi warns that due to the sensitive information processed, and the disproportionate impacts on children, people in situations of homelessness, undocumented people and other people facing social exclusion, identity cards should be used only when strictly necessary, and fully in line with EU human rights law and the *Convention on the Rights of the Child*.

Based on the methods and risks analysed in this paper, we define six key risks of the use of age verification and age estimation tools in particular, which are explained further in Chapter 4:

1. Violating children's privacy and data protection rights;
2. Infringing upon children's autonomy and self-expression online;
3. Letting companies control what children can see and do online;
4. Making anonymity online difficult or impossible;
5. Exacerbating structural discrimination; and
6. Creating a false sense of security.

Our analysis finds that there are no EU-wide **document-based verification** or **estimation** tools which minimise these risks to the extent that their widespread use could be considered compatible with children's rights in the online environment. Age **declaration** tools are more likely to be compatible with children's rights, but require further research and development into how to increase their effectiveness. For these reasons, we warn that as a general rule, **policy- and law-makers must not mandate age estimation or document-based verification measures.**

We therefore find that any law mandating providers to use age verification systems for controlling access to digital platforms and services in general – such as is proposed by the CSA Regulation – would pose an unjustifiable threat to children's digital rights and must be rejected. In particular, **document-based verification and estimation tools should not be made mandatory by the CSA Regulation, nor should their use be incentivised via the proposed risk assessment and mitigation process.**

Recommendations, codes and other policies could ensure that if specific age verification methods are demonstrated to be effective, proportionate and non-discriminatory, then they would be used in a way which is compliant with the *General Data Protection Regulation* and mitigates the risks discussed in Chapter 4. Seventeen specific recommendations are provided at the end of this briefing.

Chapter 1. Legal Context

1.1. The Charter of Fundamental Rights of the EU

The *Charter of Fundamental Rights of the EU* ('the Charter') guarantees everyone's rights and freedoms, including our fundamental rights to privacy, free expression and access to information. Children's rights to privacy, free expression and access to information are further encoded in the international *Convention on the Rights of the Child* (CRC). These rights apply online, just as they do offline, and can often function as gateways to the enjoyment of other human rights. For example, voting in the EU is always done anonymously, as it is a principle of democracy that privacy is essential for people to develop and exercise their democratic rights freely and without interference or judgement.

It is for similar reasons that, in general, we do not believe that presenting identity documents should become a mandatory precursor for involvement in public life. The risks that come with identifying people wherever they go – from having a chilling effect on people's political freedoms, to excluding those without the right documentation – can be severe. Whilst there may be specific scenarios in which disclosing identity documents may be justifiable, the widespread adoption of such practices is not justifiable in a democratic society.

These concerns are equally present when it comes to the use of age verification methods online. We challenge the premise that either children or adults should need to show formal documentation – or provide sensitive personal data – to do things like download a messaging app to contact their family. Such measures would fundamentally shift how the internet operates, as well as our relationship to the internet. There is a lack of evidence that such measures will keep children safer. On the contrary, emerging research shows that privacy and safety by design, for example having privacy features activated by default, are an effective way to safeguard children online without violating their privacy, free expression and data protection rights.[3] Crucially, these measures can achieve the same purpose of protecting children, without the restrictions on basic liberties that arise when anonymity in online spaces is no longer possible for anyone.

1.2. The General Data Protection Regulation & the Digital Services Act

The *General Data Protection Regulation* (GDPR) (2016/679) builds on the right to data protection established in the Charter, for both adults and children. It creates a range of rights for people to have knowledge of and control over the processing of their personal data, and obligations for those processing it (including digital service and platform providers).

Providers operating in the EU already frequently use forms of age declaration, whereby a user confirms their age, in order for the provider to meet their obligations under Article 8 of the GDPR. This allows children above 16 years of age to provide their own consent to the processing of their personal data when using an 'information society service' (e.g. social media or messaging app). For children below 16 years of age, the consent of their parents is required. However, EU Member

[3] For example, https://www.cnil.fr/en/cnil-publishes-8-recommendations-enhance-protection-children-online and https://www.brookings.edu/articles/using-safety-by-design-to-address-online-harms/

States can decide to set a lower limit for which parental consent can apply, which must not be below 13 years of age. Eighteen of the 27 EU Member States have done so.[4]

This means that the age at which parental consent is no longer obligatory in the EU varies between ages 13 to 16, depending on where the child and/or the provider resides. Since providers must demonstrate that the consent they have gathered is valid, the GDPR is generally interpreted as requiring some form of age verification for platforms or services that are offered directly to children.

The GDPR is an important mechanism for the protection of children's rights when it comes to age verification practices. It requires providers who process children's data to take appropriate measures to safeguard those children, but without forcing them to use a particular age verification tool. Data protection authorities can also help interpret an appropriate balance of rights when it comes to the use of age verification systems, given how many fundamental rights are at stake.

The GDPR also establishes mechanisms to admonish providers that are not sufficiently protecting children's data, including in relation to their age. For example, in September 2023, TikTok was fined €345 million by the Irish data protection authority for making the profiles of child users public by default, nudging them towards accepting settings that would not respect their privacy, and not having sufficient safeguards relating to underage users.[5] Once the *Digital Services Act* (DSA) (2022/2065), which was adopted in 2022, is in full force, there will be even more legal mechanisms at the disposal of companies and regulators to ensure that children are protected online. Article 35(j) of the DSA specifically allows providers to use age verification measures.

1.3. Necessity and proportionality assessment

As this paper will show, there are several ways in which age verification processes can severely restrict fundamental rights to privacy, data protection, access to information, free expression and association, equality and non-discrimination. In particular, we focus on children's exercise of these rights, making the threshold for what is considered necessary and proportionate even higher. However, we also note that the vast majority of the risks raised in this paper will apply just as strongly to adults too. Whilst all adults who rely on digital tools and services will be impacted, the effect will be particularly profound for those whose profession and/or safety rely on their privacy online: journalists, lawyers, human rights defenders, survivors of online (and offline) violence, sex workers, activists and others.

According to Article 52(1) of the Charter, all the above-mentioned fundamental rights can have limitations placed on them by the state. However, this limitation must always be **necessary** (meaning that the proposed measures are effective for pursuing a legitimate aim, and the intrusion is limited to the minimum needed to achieve that aim), **proportionate** (meaning that the negative consequences of the limitation do not outweigh the benefits), and must be set out in law. The burden is on the state to demonstrate, with evidence, that the restriction is necessary and proportionate.

4 https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu/consent-use-data-children

5 https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok

The analysis undertaken in this paper suggests that the principles of necessity and proportionality are unlikely to be satisfied by any widespread age verification system, with the exception of self-declarations. This is because:

- The proposed measures (document-based age verification or age estimation) are very intrusive;
- Effective alternative measures, such as privacy and safety by design, and age self-declarations exist;
- The risks to children's rights are significant; and
- The negative societal consequences of introducing widespread online age verification infrastructures are significant.

Children's rights do mean, however, that the answer cannot be to do nothing. It is essential that platforms and services take rights-respecting steps within their power, such as relating to service design and data minimisation, to protect children on their platforms.

1.4. The EU's proposed Child Sexual Abuse Regulation

Age verification rules are put forward in the EU's proposed *Child Sexual Abuse Regulation* in four key places:[6]

- Article 3.2(b) strongly encourages all **digital service providers** operating in the EU (including social media platforms, email providers and cloud services) to use document-based age verification measures. The text suggests that their risk of being issued with a 'Detection Order' (legal order requiring them to scan the communications of their users) is reduced by having such age verification measures in place;
    - This makes it likely that even platforms or services that aren't mandated to introduce document-based age verification will still choose to do so, in order to avoid penalties under the CSAR;
    - Furthermore, the rationale of the authors of the legislation is not clear: no evidence is provided to show that there is a correlation between a provider having age verification measures in place, and a reduced risk of child abuse material being disseminated.
- Article 4.3 requires private message services, including those offered via gaming platforms, to use document-based age verification or age estimation measures if they have identified a risk of grooming (which in accordance with the CSAR's risk profile is likely to be all private message services).
- Article 6 requires app stores (e.g. Google Play, Apple Store and F-Droid) to block 'child users' (under-17s) from downloading apps with a 'significant' risk of grooming (Art. 6.1(b)) and to use document-based age verification or age assessment measures for all users (Art. 6.1(c)).
- Articles 7-11 can force providers to scan for evidence of grooming in the written or audio messages or other behaviours of their users in conversations involving at least one 'child user'. Information gathered through prior age verification measures would be used to compel the providers to scan conversations where at least one person is a child user (i.e.

[6] Note that, as there are no set terms in EU law, the CSAR uses the term 'age verification' to refer specifically to document-based age verification practices.

either between a person over 17 and another under 17, or between two or more people under 17):

- This presupposes that platforms will keep an ongoing record of the ages of all of their users so that they can continually distinguish between child and adult users;
- The broader issue of why grooming detection is not a robust or rights-respecting practice, as well as EDRi's broader concerns about the CSAR, are explained in detail in EDRi's position paper, and thus are not elaborated further here.[7]

These proposed measures will create the human rights risks that are explored at length in Chapter 4. In particular, these measures would see providers mandated to process children's sensitive data to verify their age, as well as to block children's access to certain apps. Given that the proposal considers a 'significant' risk to exist at a very low threshold, it is likely that apps focused on protecting the privacy of their users – such as by refraining from collecting unnecessary data, and securing messages via encryption – would be the most likely to be blocked.

The existence of the GDPR and the DSA further questions the necessity of mandating EU-wide age verification measures, for example in the CSA Regulation. This is because age verification measures can already be implemented under the GDPR and the DSA (Art 35(j)) if they are shown to be necessary and proportionate.

[7] EDRi, 'A safe internet for all: upholding private and secure communications', October 2022, available at: https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-CSAR.pdf

Chapter 2. Categories of age verification

Although terminology is not always used consistently, we use the term '**age verification**' as an umbrella term for a wide range of methods that attempt to verify – with varying levels of confidence – the age of a particular person online. We recommend avoiding the term 'age assurance', which is a term frequently pushed by the lucrative 'age assurance' industry. In 2021, an association of industry providers estimated that by 2026-2028, the EU's age verification market would be worth almost €4 billion.[8] It seems likely that the significant financial opportunity which would be created by the widespread uptake of these tools is a motivating factor for many companies to recommend the use of such tools.

In this paper, we split the broad issue of age verification into the categories of '**declaration**' (sometimes referred to as 'age checks', 'age gates' or 'attestation'), 'document-based **verification**' (sometimes referred to as 'certification'), and '**estimation**' (sometimes referred to as 'scoring', 'assessment' or 'assurance'), under each of which numerous methods fall depending on the core functionality that they use to determine the age of a given user.[9] These terms are not definitive, but at the time of writing seem to be the best way to distinguish between broad types of methods.

***Age declaration** methods generally work by asking the user their date of birth or age bracket (e.g. 'confirm you are over 18') in order to gain access, or simply by stating (for example in terms and conditions) that certain services or features are not available to users below a certain age. Some methods ask contacts to 'vouch' for another user.*

Article 5.1(c) of the GDPR requires providers to minimise the personal data that they collect and process about their users. Read together with GDPR Article 8, it is usually interpreted that age declaration methods offer an acceptable balance – they reasonably assess age without being too intrusive or amassing sensitive data. This method is not foolproof, but the sensitivity of children's data means that regulators have rightfully been wary of encouraging providers to systematically process people's data unless it is *strictly* necessary.

In some countries and for specific purposes, for example for access to pornographic or gambling services, a small number of EU governments have required or are considering requiring providers to verify that users are over 18. Such age verification systems work by using official documentation or proxies for official documentation (for example a credit card, or by requiring people to get a proof of age code or token from a physical location, such as a shop or post office,

8 https://avpassociation.com/thought-leadership/estimating-the-size-of-the-global-age-verification-market/

9 There are other categories and methods of age verification seen in other scenarios – such as ultrasound or bone density testing of children making asylum claims – which can have very severe impacts on human rights. Such methods, however, are outside the scope of this briefing, which is limited to the main age verification methods used for online services or platforms.

which they can then enter to access online services). Such proposals have frequently been met with concerns that they are creating large surveillance infrastructures which can easily be misused or repurposed for other forms of pervasive tracking of people's digital lives.[10]

***Document-based age verification** methods generally work by requiring the user to provide an official identity document, or other age-restricted document. This may be checked manually or automatically, either by a provider, a government system (e.g. eID) or a third party.*

Whilst in theory it may be possible to have effective, rights-respecting digital ID systems for this purpose,[11] this is not currently a feasible EU-wide solution. National eIDs are not available in every EU Member State for all persons above the age of digital consent. Moreover, the planned EU-wide digital identity wallet under the eIDAS reform (the exact specifications of which are still being negotiated and therefore may not be sufficiently privacy-protective) will not be widely available for several years after the adoption of the CSA Regulation. Children without their own devices, or whose countries do not issue an eID at their age, would either be excluded or reliant on a parent or guardian's eID. For young people who are at risk of control or abuse from their parent or guardian, this could see them unable to access digital services and platforms.

The European Commission has estimated that in the best-case scenario, by 2030 the European Digital Identity Wallet will have been taken up by 80% of the eligible population, meaning a serious risk of digital exclusion for the remaining 20%.[12] Undocumented persons will never be eligible.

Given the potential risks posed by document-based age verification methods, particularly when they can tie a person's internet use to their identity, many providers have recently turned to age estimation techniques in an attempt to minimise the data that they collect and to avoid needing to rely on identity documents. This is especially relevant in the context of children's safety online, because some young people may not have formal identity documents or access to robust electronic identity tools, meaning that age estimation is already being trialled by services widely used by children, such as Instagram.

***Age estimation** methods generally work by using data about the user, combined with predictive analytics (such as facial analysis or other AI-based tools), to guess their age. It may be based on the user's appearance, on their online preferences or internet history.*

These estimation methods, however, can be inaccurate, discriminatory and deeply invasive. Those such as UK-based 'age assurance' company Yoti, claim, for example, to be GDPR-compliant

---

10 See, for example: https://www.theverge.com/23721306/online-age-verification-privacy-laws-child-safety and https://www.theguardian.com/australia-news/2023/aug/31/roadmap-for-age-verification-online-pornographic-material-adult-websites-australia-law

11 The French data protection authority has described a proof of concept for what a privacy-preserving age verification system could look like. However, the system is not currently functional, nor does it resolve many of the issues raised in this paper, such as structural exclusion or legal necessity. Available at: https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process

12 https://www.biometricupdate.com/202305/universal-global-digital-identity-still-7-years-away-oix-presenter-says

because they don't process biometric data for identification purposes (meaning that they only use the scan of the user's face to estimate their age, not to identify or recognise the user). We believe this claim to be misleading, as the tools used clearly have the capacity to identify the person.

Age estimation practices may also amount to prohibited automated profiling under Article 22 of the GDPR. Article 22 of the GDPR does make an exception for profiling on the basis of explicit consent (Art 22.2(c)). However, it is questionable whether children using such methods are truly consenting, given the lack of awareness of the potential consequences of this processing. There is also the fact that their consent may not be freely given because it is, in practice, required for them to access online platforms such as message services or social media.

Chapter 3. Analysis of key methods

3.1. Overview & summary table

In terms of how robust age verification measures are, only **document-based age verification** methods can be assumed to have a reasonably high level of accuracy – although even then, this can be circumvented by using someone else's documents. They can also be very invasive, and come with significant risks. There is also a practical problem: in this research, we have not found any current or reasonably foreseeable document-based verification method which is available across the EU and which would meet human rights requirements. The French data protection authority, the CNIL, has found that whilst it is in theory possible to create a pseudonymous age verification system, it does not currently exist.[13] Any foreseeable solution could also be circumvented by a VPN, their researchers add.[14]

Age declaration is easier to spoof, yet generally poses far fewer risks for both child and adult users. As the French authority, the CNIL, points out, complementing age declaration with age-appropriate design as well as non-technical measures – for example, parental supervision – can make age declaration methods suitable in many cases.[15] This fact has also been emphasised in the European Parliament's Internal Markets Committee opinion on the CSA Regulation (Recital 16b).

Age estimation methods in general seem unlikely to be sufficiently accurate, often having a margin of error of several years, especially for people of colour. They are very intrusive and encourage the mass collection of personal data and large-scale profiling. Facial recognition methods can also be easily circumvented by using a friend or relative for enrolment. This problem could be avoided by requiring checks each time a person logs on, but this would incentivise the routine processing of sensitive data as a result, and might even incentivise the creation of underlying biometric databases of children – posing a clearly unacceptable risk.

What this section most hopes to emphasise, therefore, is that **there is no silver bullet for age verification.** Furthermore, **there is usually a trade-off between invasiveness and risk on the one hand, and effectiveness on the other.** The most theoretically effective measures may fail to meet the necessary threshold to protect young people's sensitive data, and pose broader risks of exclusion and surveillance. The rights-respecting methods may not give enough confidence in their outcomes unless they are supplemented with other, (often non-technical) measures. **This is a currently unsolved problem for both providers and legislators.**

There may also be an issue of an over-focus by policy-makers on age verification and an over-estimation of its purported benefits. For example, as the children's digital rights group 5Rights Foundation points out, 'effective risk mitigation can on the contrary nullify the need for age assurance'.[16] By disincentivising the need for children to give a false age through better service

[13] https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process
[14] https://www.theverge.com/23721306/online-age-verification-privacy-laws-child-safety
[15] https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors
[16] Input to the European Commission consultation on the Child Sexual Abuse Regulation by 5Rights Foundation: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Fighting-child-sexual-abuse-

design and appropriate parental oversight, potentially harmful age verification measures, like document-based verification, may not be needed.

The following table compares methods for age verification during sign-up to online services and platforms on a general basis (i.e. as proposed by the EU's CSA Regulation) rather than for a specific service (e.g. gambling). The criteria against which we have assessed the categories and methods are:

- **Invasiveness** = does it require (or even incentivise) a lot of data collection and processing, particularly sensitive data, and treat it in ways that could harm the user?
- **Effectiveness** = does it accurately and robustly assess the age of the person in the context of online platforms and services? Is it easy to circumvent/spoof? Can it be accessed/used by everyone that should be able to access digital services and platforms?
- **Risk level** = what risk does it pose to the fundamental rights and freedoms of all internet users, especially children? Does it risk excluding people (above the requisite age), for example because they are unable to meet the age verification requirements (access to eID or physical identity documents) or because they are unwilling to do so because of loss of anonymity online or other chilling effects?

Please note that whilst this table summarises eleven methods of age verification that we have identified and classified within three broad categories, it is not exhaustive. It is intended to represent the most common methods.

Method	Invasiveness	Effective-ness	Risk level	Conclusion
Age declaration				
1: Implicit declaration via terms and conditions	Low	Low	Low	Limited usefulness
2: Self-declaration of being above a certain age threshold	Low	Low to medium	Low	Promising, but needs to be bolstered with other measures
3: Self-declaration of date of birth	Low	Low to medium	Low to medium	Method 2 is preferable
4. Social vouching	Low to medium	Low	Low to medium	Do not recommend
Document-based age verification				
5: Upload official documentation to provider or third party	Very high	Medium	Very high	Do not recommend
6: Use official documentation to create a token (by provider or third party)	High	Medium	High to very high	Do not recommend. Further research needed.
7. Use of proxy for official documentation (e.g. student card, credit/debit card)	Medium to high	Low	Low to medium	Do not recommend

detection-removal-and-reporting-of-illegal-content-online/F3337920_en

8: Use national or international digital ID system (eID) to create a token	Low to high, depending on architecture	High in theory; low in current and foreseeable forms	High	Do not recommend. Further research needed
Age estimation				
9: Use facial analysis or other AI to predict the age of the user	Very high	Low-medium	Very high	Do not recommend
10: Use other data to predict the age of the user	Very high	Low-medium	Very high	Do not recommend
11: Requiring users to perform a task or activity to 'prove' their age	Low	Low	High	Do not recommend

3.2. Category: Age declaration

These methods are attractive because they are simple, largely non-invasive, and easy for providers to apply in order to meet their requirements to specifically protect the data of users aged between 13 and 16, and to prevent subscription by under-13s (Article 8 of the GDPR). The exception is method 4, which creates a dependency on other people that could disempower the user requesting the age check.

Method 1 on its own is not robust enough, and methods 2 and 3 may require additional design or supervision measures. Therefore they do not stand alone, but require a more holistic approach to online safety which also focuses on design and supervision – otherwise children may be incentivised to enter a false age. As discussed in section 1.1, with such additions, age declaration method 2 is likely to be suitable for most general online age verification use cases. Note: from a data protection perspective, it is less risky for the provider to ask the user to choose an age bracket (i.e. method 2), rather than to provide specific information about their date of birth (method 3). However, neither method contains any way of validating the information.

Method 1: Implicit declaration by describing age restrictions in the terms of service or community guidelines

Pros	Cons	Risks
Simple	Passive and therefore easy to ignore or overlook	None significant
	Unlikely to meet requirements for GDPR Article 8 on its own (would need to be combined with another method)	

Method 2: Self-declaration of being above a certain age threshold (e.g. I am 'over 13', 'over 16' or 'over 18')

Pros	Cons	Risks
Simple	Difficult to prevent false declarations	Provider could use age bracket to target advertising
Cheap to apply	False declarations could create issues of data accuracy, which could be an issue for GDPR Article 5 (personal data must be accurate) and lawfulness of processing (consent is invalid if given by a child below the	

	age of consent)	
Not invasive		
Generally understood to allow providers to fulfil their obligation with Article 8 of the GDPR (children's data), although may rely on other mechanisms such as age-appropriate design and parental supervision		
Compatible with Article 5.1(c) of the GDPR (data minimisation)		
Allows users to remain anonymous, which is important for enjoying a wide range of human rights online		

Method 3: Self-declaration of date of birth

Pros	**Cons**	**Risks**
Simple	Difficult to prevent false declarations	Provider might unnecessarily retain sensitive birth date data
Cheap to apply	Could create issues when it comes to Article 5.1(c) of the GDPR (data minimisation)	Provider could use this to target advertising or to sell to a third party
Not very invasive	False declarations could create issues of data accuracy, which could be an issue for GDPR (see method 2)	
Allows users to remain anonymous, which is important for enjoying a wide range of human rights online		
Likely to meet requirement of Article 8 GDPR (children's data)		

Method 4: Social vouching (asking other users to confirm whether a person is under or over 18)

Pros	**Cons**	**Risks**
	Relies on people having connections to friends or relatives who know them in real life and are active on the platform or service	Makes people's internet use contingent on others, which can harm their dignity and autonomy
	Can take a long time to get a response	
	Errors could create issues of data accuracy, which could be an issue for GDPR Article 5 and the lawfulness of processing (if the child is below the age of consent, only parents or guardians can give valid consent for processing of personal data of the child)	

3.3. Category: Document-based age verification

As document-based age verification methods rely on some form of identity document, they require the declaration of sensitive information to a provider or a third party (which could be a government or a commercial entity like Yoti) by design (all methods). This creates inherent risks both of deliberate misuse of data for surveillance or advertising purposes, as well as risks of the data being hacked. leaked to third parties, or exploited for identity theft and fraud. Given that a lot of EDRi's work in recent years has been

focused on systemic violations of people's data by online providers as well as by governments, we have good reason to be wary about these systems.

There is also a risk of exclusion on the basis of nationality or other characteristics. This is because some countries do not have national digital identity systems, and even countries that do, do not have uniform coverage (passports are generally only needed for international travel outside the EU). It's particularly a problem given that the main need here is to separate children from adults: some Member States' national IDs are only for over 16s or over 18s, which means that the requirement of Article 8, to distinguish children aged 13-16, might be hard to meet. There is also the fact that undocumented people, and communities that face high levels of structural discrimination, such as Roma and Sinti people, may not have access to any identity documents, locking them out of digital services. The use of proxies (method 7), such as credit cards or student cards, is ineffective and does not solve the problem of exclusion.

It is theoretically possible that a future digital identity system (method 8) which is widely available, which is able to verify ages in a genuinely anonymous and permanently untraceable way, and which fully respects privacy and data protection, could be used widely. However, such an infrastructure is not currently confirmed, even for the EU's digital identity wallet, which may or may not adhere to these standards, depending on the final trilogue agreement. It would also not address the issue of structural exclusion of those without identity documents, which poses a severe risk to such individuals.

To be acceptable, an age verification system would need to:

- *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');*
- *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;*
- *Not allow any data collected or processed to be used for any other purpose;*
- *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;*
- *Be robust and secure from a cybersecurity perspective;*
- *Be consensual, and not overly burdensome for those who do not want or do not have the means to verify their identity in this way;*
- *Be used only where strictly necessary;*
- *Be 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.*

Method 5: Uploading a scan or photo of passport, national ID or other official proof-of-age document to the provider or a third party

Pros	Cons	Risks
Allows the provider to check the user's self-declared date of birth against an official ID document. This means that circumvention and spoofing are more difficult because they require modifications of the digital copy. On the other hand, unless the verification requirement is global,	Very invasive, especially if the provider is checking the document against other parts of the account	Discrimination against those who do not have an identity document, in particular likely to harm those who already face high levels of structural discrimination (undocumented people, asylum seekers, Roma and Sinti communities – including children from all these communities),

the entire verification process can be circumvented with a VPN.		leading to an exacerbation of social exclusion
In theory relies on an officially-validated document, so the age should be accurate	Not everyone has identity documents.	Putting certain communities at a high risk, for example sex workers who have been shown to be put at higher risk of exploitation through these measures
	Requires user to trust a private/commercial entity with their ID document	Making it difficult for anyone to be anonymous online, including people whose safety relies on this (journalists, whistleblowers, people who have experienced online harassment or abuse)
	Puts all of this sensitive data in the hands of Big Tech, the opposite of what laws like the DSA are trying to achieve	Creating the possibility of tracking each person's internet use and linking it to their legal identity, which creates conditions for surveillance and data retention
	As some countries do not currently provide ID documents to children of all relevant ages, it would prevent granularity (i.e. this method could only be used for cross-border services to prove that a user is over 18). It could also motivate countries to issue IDs to children.	High risk of misuse of very sensitive data for advertising or selling to third parties
	Needs to be individually checked, so is very resource-intensive (unless it uses AI, which creates its own problems of (in)accuracy and a risk of automated profiling)	Keeping so much sensitive data in one place can incentivise hacks. If hacked, this can create risks of identity fraud
	Every person needs to identify themselves in order to use the platform/service, which can discourage some people	
	Very unlikely to be compatible with Article 5.1(c) of the GDPR (data minimisation) because it systematically requires the sharing of unnecessary data. It would only be necessary to know if the user is above or below an age threshold, but the user has to provide a lot of sensitive information about themselves.	
	Scans/uploads can be spoofed or digitally altered	
	Normalises needing an ID document to take part in day-to-day life	

Method 6: Uploading a scan or photo, or performing a video capture, of a passport, national ID or other official identity document to a third party, which then provides a token to the provider to confirm the age bracket of the user (e.g. 'above 13' or 'above 18')

Pros	Cons	Risks
Relatively difficult to circumvent/spoof (same as method 5). On the other hand, unless the verification requirement is global, the entire verification process can be circumvented with a VPN.	Possible for young people to use each other's tokens, or to use a parent/relative's ID to create a token, reducing effectiveness	Discrimination against those who do not have an identity document, in particular likely to harm those who already face high levels of structural discrimination (undocumented people, asylum seekers, Roma and Sinti communities – including children from all these communities), leading to an exacerbation of social

		exclusion
Token makes it less likely for the internet activity to be linked to the legal identity	Relatively invasive (although the exact architecture of the system has the possibility to minimise this)	Making it harder for anyone to be anonymous online, including people whose safety relies on this (journalists, whistleblowers, people who have experienced online harassment or abuse, sex workers, etc.)
If tokens are issued as single-use for each online platform, the tokens cannot be used to track users across platforms	Relies on trusting the third party, often based on promises rather than transparency and verifiability	Creating the possibility of tracking each person's internet use and linking it to their legal identity, which creates conditions for surveillance and data retention
	Not everyone has identity documents	Possible risk of misuse of very sensitive data for advertising or selling to third parties
	Requires user to trust a private/commercial entity with their ID document	If data are stored, the keeping of lots of sensitive data in one place can incentivise hacks. If hacked, this can create risks of identity fraud.
	As some countries do not currently provide ID documents to children of all relevant ages, it would prevent granularity (i.e. this method could only be used for cross-border services to prove that a user is over 18)	Some deployments of it have been combined with biometric identification or verification systems, encouraging the uptake of biometrics
	Expensive for providers, which can discourage uptake (and be impossible for small or open-source providers)	
	Every person needs to have and be willing to share their legal identity in order to use the platform/service	Researchers have shown that such methods are very vulnerable to hacks[17]
	Puts all of this sensitive data in the hands of private companies. This is not independent, and it will be incentivised by profit	
	Risk of incompatibility with Article 5.1(c) of the GDPR (data minimisation)	
	If no alternative, could violate requirement for consent under the GDPR (if that's the basis that the provider has chosen to use)	
	Scans/uploads can be spoofed or digitally altered	
	Normalises needing an ID document to take part in day-to-day life	

Method 7: Use of proxy for official documentation (e.g. student card, credit/debit card)

Pros	Cons	Risks
	Easy to spoof	Creates conditions where those who can use this method are chosen at best arbitrarily, and at worst in a discriminatory way
	Different countries allow credit or debit cards to be issued at different ages, so does not offer an EU-wide solution	
	Privileges those with specific	

[17] https://www.golem.de/news/manipulierte-ausweise-ccc-macht-videoident-kaputt-2208-167530.html

	education or financial situations	
	Risk of incompatibility with Article 5.1(c) of the GDPR (data minimisation) depending on the documentation chosen, as it may reveal additional sensitive information about the person.	

Method 8: Using a national or international 'eID'/digital identity system which then provides a token to the provider to confirm the age of the user

Pros	Cons	Risks
In theory, difficult to circumvent/spoof. However, cyber researchers have already demonstrated the risk of identity theft and fraud with these methods (see 'Risks' column).	Currently not available uniformly (i.e. not in all countries) so cannot function as an EU-wide solution, only a national solution	Discrimination against those who do not have an identity document (which is a precondition for getting access to an eID), in particular likely to harm those who already face high levels of structural discrimination (undocumented people, asylum seekers, Roma and Sinti communities – including children from all these communities), leading to an exacerbation of social exclusion
Theoretically does not link internet activity to legal identity (although the EU's future digital identity wallet (eID) may allow users to be de-anonymised)	Where available, can be quite 'buggy' as technologies are not always mature or reliable	Discrimination on the basis of nationality (i.e. only people from certain countries would have access)
Plans for an EU-wide eID to be in operation only in the late 2020s (currently the EU hopes that there will be 80% adoption by 2030)	Creates possibility for government to track all internet use; relies on being able to trust government not to surveil internet activity (which is currently a genuine risk for the EU-wide 'solution')	Making it very difficult for anyone to be anonymous online, including people whose safety relies on this (journalists, whistleblowers, people who have experienced online harassment or abuse, sex workers, etc.)
	Relies on the eID design being 'zero knowledge' and without any tracking, which is not the case currently for the EU-wide eID	Creating the possibility to track each person's internet use and link it to their legal identity, which creates conditions for surveillance and data retention
	If no alternative, could violate requirement for consent under the GDPR (if that's the basis that the provider has chosen to use)	Keeping so much sensitive data in one place can incentivise hacks. If hacked, this can create risks of identity fraud
	Government-held does not mean the data are necessarily secure	The EU-wide eID is never expected to have full coverage across the EU, meaning an ongoing risk of digital exclusion
	As some countries do not currently provide eIDs to children, it would prevent granularity (i.e. this method could only be used for cross-border services to prove that a user is over 18). In the BIK+ communication [COM(2022) 212 final], the Commission notes this limitation of eIDs for the age verification of children, and says that it will work with Member States to get them to issue eIDs to children.	Researchers have demonstrated that these systems can make people vulnerable to identity theft and data theft.[18]
	If children have to rely on the eID of	

[18] https://lilithwittmann.medium.com/mit-der-id-wallet-kannst-du-alles-und-jeder-sein-au%C3%9Fer-du-musst-dich-ausweisen-829293739fa0

	their parent or guardian, this could put children whose parents or guardians control, abuse or exploit that at even greater risk, by making their internet access contingent on an abusive parent/guardian	
	Normalises needing a digital ID document to take part in day-to-day life, and can create a chilling effect.	

3.4. Category: Age estimation

Assessment of age estimation methods:

Age estimation methods (9 and 10) are deeply problematic by design, as they rely on having sufficient amounts of data about the user in order to make their estimation. In the wider context of surveillance capitalism, and considering that the EU's Digital Services Act forbids providers from targeting online advertisements towards children, age estimation measures could therefore be seen as incompatible with the EU's approach to protecting children online.

There is also not only a risk of stereotyping people in a harmful way, but actually forcing a provider to define what they might consider to be 'acceptable' or 'normal' behaviour for children and teenagers compared to adults. This is a complex sociological question, and not one that can be easily translated into a technological tool. Method 11, for example, also shows extreme potential for discrimination against people with disabilities and neurodivergent people.

Furthermore, age estimation methods intrinsically rely on predictions, rather than certainty, which can create issues for data accuracy, as well as how to deal with the inevitably high level of users that will be estimated as older than they truly are, or younger than they truly are. This could mean that adults could be allowed into supposedly child-only spaces, or that adults, or older teenagers, could be locked out of spaces that they are supposed to be able to access. Putting the burden on them to rectify this can, in and of itself, suppress some people's free expression.

The predictive nature of these systems may also create a problem under Article 22 of the GDPR, which is supposed to stop profiling unless there is explicit consent – which section 1.1 of this briefing shows is unlikely to be the case here. Moreover, the idea of private companies using children's faces to profile them in order to decide whether or not they can access a service or a space is worrying in the wider context of abuses of biometric data by both private and state entities.[19] With the EU's Artificial Intelligence (AI) Act still under negotiation at the time of publication, practices which use AI to profile or categorise people based on their faces or other body parts or characteristics could be further restricted or even prohibited in the EU.

Method 9: Using facial analysis or other AI-based tools to predict the age of the person

Pros	Cons	Risks
Doesn't require legal identity, so lower risk of exclusion for those without identity documents	Deeply invasive	Likely to create systemic discrimination as AI-based tools are not uniformly reliable, and repeatedly show that they are not reliable with certain demographics
Available across the EU	Facial recognition or other AI-based age predictions/estimations are not sufficiently reliable for a context	Likely to fail children who are close to an age threshold, because these systems are at best accurate within a

19 https://edri.org/our-work/blog-ban-biometric-mass-surveillance/

	where determining age accurately is important. EDRi has long opposed the systematic use of biometric data for such purposes, warning that this creates the infrastructure for biometric mass surveillance practices.	threshold of 2-4 years. Could shut children out of services or information, as well as adults who appear youthful
	Requires the systematic processing of very sensitive data of all users, including children (and thus also likely to violate GDPR Article 9)	May reveal other information or characteristics that could be used to target advertising or for other unacceptable purposes
	Especially likely to be unreliable for black, brown and Asian people, as well as people with certain disabilities	Keeping so much sensitive data in one place can incentivise hacks. If hacked, this can create risks of identity fraud.
	Easy to spoof/circumvent by presenting another person	Risk of allowing underage children into spaces not intended for them
	Whether it is the provider or the third party, this is exactly the sort of data collection that the DSA and AI Act are supposed to minimise	Can lead to a normalisation of biometric online checks (as seen in China)[20] without proper understanding of the risks and consequences, for example surveillance or identity theft
	May violate Article 22 of the GDPR (profiling)	
	Errors could create issues of data accuracy, which could be an issue for GDPR Article 16 (right to rectification)	

Method 10: Using other data to predict or verify the age of the person

Pros	**Cons**	**Risks**
Doesn't require legal identity, so lower risk of exclusion for those without identity documents	Relies on underlying profiles about each user	Incentivises mass data collection, retention and analysis of children's data by platforms
Available across the EU	Can reveal very sensitive information. EDRi has advocated for a ban on the categorisation of people on the basis of sensitive characteristics, including age, using their biometric data, which was adopted as the position of the European Parliament in 2023.[21]	Lots of evidence of these sorts of profiles being used to manipulate people's purchases, exclude them from certain jobs, radicalise them, or influence how they vote[22]
	Won't work for people with a limited internet footprint or who have more stringent privacy settings	Incentivises profiling of children
	Based on stereotypes	High risk of discrimination
	Some providers are known to use invasive methods to verify the user's self-declared date of birth, such as scanning social media posts and maybe even private messages for birthday greetings[23]	
	Relies on pre-defining the sorts of behaviours that the platform considers represent a child vs. an adult, which may lack cultural or other context	

20 https://www.bbc.com/news/world-asia-china-50587098
21 https://edri.org/our-work/european-parliament-draws-red-line-against-biometric-surveillance-society/
22 https://edri.org/our-work/surveillance-based-advertising-an-industry-broken-by-design-and-by-default/

	May violate Article 22 of the GDPR (profiling) and Article 5.1(c) (data minimisation)	
	Exactly the sort of data collection that the DSA and AI Act are supposed to minimise	
	Errors could create issues of data accuracy, which could be an issue for GDPR Article 16 (right to rectification)	

Method 11: Task-based

Pros	**Cons**	**Risks**
Doesn't require legal identity, so lower risk of exclusion for those without identity documents	There is no standard measure of what tasks a child or an adult can do, so this will always be based on stereotypes and assumptions	Discrimination against and exclusion of people with physical and intellectual disabilities as well as neurodivergent people
Potentially less invasive – not about who you are, what you look like or your preferences, but rather a specific, one-off task	This can easily be circumvented by asking, for example, an older sibling or searching online for solutions to the task or activity	
Available across the EU	High margin of error, which matters when the whole purpose of these systems is to assess age	
	This low accuracy could create problems under GDPR Article 16 (right to rectification)	

[23] https://www.theverge.com/2022/6/23/23179752/instagram-age-verification-ai-social-vouching-methods

Chapter 4. Key human rights risks

4.1. Violating children's privacy and data protection rights

The vast majority of the methods discussed above, in particular age estimation and document-based age verification methods, rely on – and even encourage – the widespread collection, processing and in some cases, retention, of the data of children and adults alike. As children are themain target of these tools, this can constitute a serious breach of the rights to privacy and data protection for children as well as for adults. The use of biometric data for this purpose, whether or not it uniquely identifies people, can never be considered necessary given the sensitivity of these data.[24]

When combined with methods like facial analysis (method 9), this can amount to the systematic processing and profiling of children's most sensitive data. Given the sensitivity of biometric and biometrics-based data (*the latter term increasingly being used to cover systems with equivalent human rights risks but without uniquely identifying data subjects*), these methods should be seen as unnecessarily intrusive and deeply inappropriate for routine use by children.

Despite supplier claims to the contrary, many age verification systems are likely to violate the GDPR, in particular Articles 5.1(c) (data minimisation), 9 (protection of biometric data) and 22 (protection from automated profiling). Given the specific vulnerabilities of children, and that children have a necessary right to explore and express themselves both online and offline, their data are usually understood as requiring even higher safeguards than those of adult users (although it's worth noting that these methods also violate the privacy and data protection rights of adults).

As such, we would see (at a minimum) methods 5 (document-based verification), and 9 and 10 (both estimation) as unacceptable when it comes to protecting children's privacy and data, no matter what safeguards might be put in place. Other methods, such as 6 and 8 (both document-based verification), are still very risky but – as explained above – may have the potential to be made compliant with children's privacy and data protection rights in the future. This is why methods like 2 and 3 (age declaration methods) can already be considered more likely to meet requirements to protect children's privacy and data. However, if they are not combined with other measures to reduce the risk of inaccurate data, they may violate the accuracy requirement under GDPR Article 5.1(d) and the requirement to demonstrate that user consent is valid (Article 7).

Where providers are using consent as the basis to perform age verification, they will need to ensure that the person is properly informed, and has a genuine option to say no. However, given the centrality of social media and messaging apps to the lives of many children around the world, it is questionable whether they can truly say no to the measures that are offered to them.

Moreover, it may be hard for a child to fully understand what they are consenting to. Even for adults, the risks of the processing of biometric data, or problems of profiling and manipulation by

[24] https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

Big Tech platforms, are not well known. It is arguable whether we can expect a child – especially a younger child – to know the potential consequences of giving access to such data.

4.2. Infringing upon children's autonomy and self-expression online

By placing age verification barriers in the way of what children can access online, they may be physically prevented from accessing certain content or services that they should in fact be able to access. Or, they could be made to feel 'bad' or 'weird' for accessing content or services that are legitimate – and perhaps even necessary for their self-expression and access to information. This is likely to especially impact content related to sex and sexuality education, sexual health information, and reproductive healthcare, which can be very important for children to access – but may not always be supported by parents or wider cultures.

In some countries, access to such information is even criminalised, and any measure which could reveal that a young person has accessed that content could put them in danger. Because the internet is global, measures that are brought in in the EU, for example, could be forced onto other jurisdictions where children could be seriously harmed by these measures. Even where they are supported, children (rightly) might want to keep this access private.

There is an issue that 'children' as a homogeneous block is not a helpful term. Although according to international child rights law, a child is anyone under 18, there is a clear difference in what would be appropriate for a child of eight, compared to a child of twelve, compared again to a child of sixteen or seventeen. The GDPR has special protections for children of all ages, while allowing children above 13-16 years (depending on their Member State) to give consent on their own, in line with the growing autonomy of older children. Across EU Member States, the age of sexual consent ranges from 13 to 17. Therefore, some online activities that could be perfectly lawful for a 14-year-old in one EU country would be unlawful for a child of the same age in a different EU country, yet age estimation systems would still treat both as children. This is a level of granularity and nuance that is very hard for providers to assess without having access to a much broader amount of data about children's country of residence – which then creates yet more risks.

There is also a broader problem that age verification measures need to be based on a prior assessment that certain content is appropriate for children, and certain content is not. Whilst this may be true, it is far from a universal standard. What is seen as appropriate by one parent may not be seen as appropriate by another parent. It can therefore greatly harm children's growth and autonomy to set a generic standard of what they can and cannot do online.

Furthermore, parents are not an infallible authority on what is or is not appropriate – a parent trying to stop their 15-year-old child from accessing content which could help them explore their sexuality could cause a lot of harm to that child and violate their autonomy. In such cases, the fact that age declaration methods can be circumvented with relative ease can actually be a positive thing, because it can allow children (especially adolescents) to make their own decisions about what they should see. This is why organisations like the Child Rights International Network (CRIN) point to the primary importance of empowerment and resilience of young people, as well as having a trusted adult to turn to in the event that something is wrong.

They explain that this is better than any tool or technology which is supposedly designed to keep children safe (and can often instead lead to surveillance).[25]

An additional risk arises from the fact that in some cases, children may be at risk from their own parent or guardian. For several of the document-based age verification methods explored, and especially method 8, adolescents without their own formal identity documents might be encouraged to receive verification from their parent or guardian's eID wallet. This would make young people's access to some online services and platforms contingent on the abusive or controlling parent or guardian. In turn, this could actually put them at more risk of abuse or other harm. Parents or guardians could also feign 'vouching' for their child, giving them access to a child account.

Even when content might be designed only for over-18s, we also need to ask whether it is proportionate to go so far as to block children's access to that content. For example, some parents will decide that they are happy for their teenage children to watch movies rated '18'. Other content might not be intended for children, but it could be fine for them to access it. And still other content that would be proportionate when blocked for a 14-year-old might be disproportionate when blocked for a 16-year-old. This is very complex, whereas age verification is a blunt tool.

4.3. Letting companies control what children can see and do online

Another issue is the irrational premise that it is feasible and effective to 'child-proof' the internet. However, as discussed in section 2.2, there is no universal child user, nor a universal standard for what is and is not acceptable for children. This lack of universality of what is and isn't appropriate for children creates a problem. Providers that are required to implement age verification have to make an ideological decision about what they think is and is not appropriate, and need to make sure that it will translate across contexts and cultures.

Given that this is an impossible task, they may be likely to go with the highest common denominator: being maximally restrictive about what children can see and do, and restricting those children's access to content that is lawful for them. Or, conversely, they may feed children with content relating to eating disorders, suicide and other dangerous topics because the algorithms that underpin their platforms feed off attention. Either way, this gives providers – in particular Big Tech platforms – a dangerous amount of control over what children can see and do online.

These risks are particularly prevalent in well-meaning but often deeply misguided demands for platforms to stop children from being able to access 'harmful' content. Whilst everyone should be protected from manipulation and exploitation online, not everything that is harmful is necessarily unacceptable. It can be important for children to be exposed to some level of harmful or inappropriate content online, as this can build their resilience. Preventing them from doing so, by virtue of an artificially child-proofed internet, can take away children's opportunities for exploration and self-development online. When they turn 18, they risk going from a sheltered digital environment into the realities of the rest of the internet, without the tools to know how to safely navigate this. It is important, therefore, that parents/guardians and educators support children to know *how* to deal with difficult or harmful experiences online.

[25] https://home.crin.org/issues/digital-rights/childrens-right-digital-age?rq=digital%20age

Moreover, due to the problems of classifying harmful content (because it is not defined in law), recommender systems seeking to block harmful content for children are likely to exclude broad categories of content that are not harmful, just to be on the safe side. This has already been seen with lawful LGBTQI+ content posted on social media platforms. If children cannot turn off such overly broad content filters, it can unduly impact their right to information.

The *Convention on the Rights of the Child* establishes that the primary responsibility for children's upbringing is their parent(s) or guardian(s). As the UN emphasises, states must enable parents and guardians to fulfill this role.[26] Mandatory age verification, however, would see parental oversight and involvement effectively outsourced to companies. By making such practices mandatory at EU level, for example, legislators would be undermining parental involvement and thus failing to meet their obligation to parents and guardians, by enforcing a process which passes responsibility over to a private company. This disempowers both the child and the role of the parent or guardian.

This issue also points to broader normative questions about the internet and society. From its inception, the internet was conceived of as a free and open space for knowledge exchange and community building. As we have repeatedly criticised in our work on the Digital Services Act (DSA), the surveillance models of Big Tech companies and the 'walled gardens' of social media platforms have in recent years centralised their power and control over digital spaces and our digital lives.[27] Toxic business models mean that companies profit from outrage and harm, whilst people are manipulated, exploited and their privacy and data repeatedly violated by surveillance advertising, algorithmic recommender systems and other harmful practices. The answer to these problems should not be to further concentrate the power of these companies over our lives through age verification systems, but rather to replace surveillance-based business models with internet ecosystems which are based on community standards, open, democratic principles, accountability, and user empowerment and control.

4.4 Making anonymity online difficult or impossible

Age verification measures (methods 5, 6, 7 and 8), and in some cases, age estimation measures (such as method 9, which processes biometric data that can be used to identify people, or method 10, which can create a detailed portrait of your online life) pose a serious risk of making anonymity online impossible. This is because they create the possibility – in some cases, the inevitability – of connecting your legal identity to everything that you do online.

Since for some people being anonymous online is incredibly important, very serious problems can arise as a result. Being known and followed online can be incredibly dangerous for journalists and anti-corruption activists seeking information; for human rights defenders and activists challenging power; for whistle-blowers and sources whose safety depends on staying confidential; for sex workers who can be at a high risk of violence or abuse when their identity is known; for marginalised communities who have faced offline and online harassment or abuse; and for survivors of child sexual abuse or domestic abuse. Beyond that, privacy and anonymity are a pillar of democracy and an enabler of our human rights.

[26] https://www.unicef.org/montenegro/en/parenting-0
[27] https://edri.org/our-work/digital-service-act-document-pool/

Widespread age verification would also completely undermine, for example, services like Tor ('the onion router') if they were required to implement it. Tor is heavily relied on by people in countries with high levels of internet censorship, control and shutdown, and is used by journalists, human rights defenders and others as a means to stay online despite the actions of repressive states.

As discussed in Chapter 1, that is not to say that age verification could never be done in a rights-compliant way in the future. It is already less harmful to use tokens (like in methods 6 and 8) and to near-instantly delete all personal data, than it is to require people to provide scans of identity documents, especially if they are retained. However, these methods are not currently available for EU-wide use, nor are they likely to be for several more years. Furthermore, a lot more regulatory oversight and scrutiny would be needed to ensure that these methods are being performed properly and not opening thedoor for pervasive tracking and other harms. We are sceptical about whether a solution that meets all of these criteria would ever be widely implemented.

4.5. Exacerbating structural discrimination

Many people do not have official identity documents, or other documents that they can use as a proxy for an adult identity document (such as a credit card or student card – although these are problematic as they do not confirm age in the way that government-issued documents do, are available at different ages in certain EU Member States, and also have higher risks of being circumvented, so are less effective). This is likely to disproportionately affect those people who already face the highest levels of structural and social exclusion. For example, undocumented people – including, of course, undocumented children – and asylum seekers (who in some countries are not provided with formal documentation until they are granted asylum) could find themselves completely shut out of the internet. The harm of preventing a child in this situation from using a messaging service to contact their loved ones, for example, is profound and must be prevented.

In addition, some people do not have an official ID because of economic reasons (for example, people in poverty may not be able to afford a passport) or because of structural discrimination (for example, some Roma and Sinti communities who have been denied access to public services or made to feel less able to claim them). Any system that relies on having formal documentation can therefore be an economic or social barrier to people in these situations – which then serves to exacerbate the digital divide between those who can freely access digital services, on the one hand, and those who are systematically denied, on the other.

Even among those who do have official identity documents, not everyone will have access to an eID. This can lead to discrimination on the basis of nationality (because some nationalities do not have access to eID) or other criteria (such as age, since older people may be less comfortable or able to use digital methods).

Furthermore, for those who do have access to an eID, there may be good reasons why they do not feel comfortable linking their ID to their internet use. Sex workers, for example, increasingly rely on internet services to do their work. However, they face systematic exploitation from platforms, discrimination from governments and sometimes violence and abuse. As sex workers often have intersectional identities (such as being trans or undocumented), the risks to them can be even more compounded. Yet without being willing to undergo age verification (method 5, for example,

has been used by several sex work platforms) they could lose their livelihood. More broadly, anyone wanting to use the internet could experience a 'chilling effect', whereby the fear of having their internet history and communications connected to their identity would discourage them from using such services or platforms.

Another facet of discrimination that can arise is in the use of task-based age estimation methods (method 11). Asking someone to perform a task to 'prove' their age will always rely on stereotypes about what people of a certain age can or cannot do. But this is not always accessible for people with a physical disability who use a screen reader or other assistive tech. For people with intellectual disabilities or who are neurodivergent, these tasks could be highly discriminatory, and therefore likely to exclude those who do not perform the task as the provider might expect a 'standard' child or adult to do.

4.6. Creating a false sense of security

All of the methods discussed are, to a greater or lesser extent, able to be circumvented. Unless people are communicating solely with those already known to them, there can be no guarantees that a person is the age they claim to be.

This creates a risk that spaces which appear to be accessible only to children can in fact be exploited by malicious actors. If children, and the adults supervising them, believe that age verification tools have stopped adults from entering a certain space, this can create a false sense of security. In section 4.2, for example, we highlighted that parents or guardians could use eID systems to create accounts pretending to be their child, which could allow abusers who are also parents/guardians to target other children. Thus, instead of being alert to risks – as we all should be when communicating with people online whom we do not know – children may believe that they are amongst peers and so can let their guard down. This could make them more vulnerable to grooming and other forms of exploitation.

In fact, in a counter-intuitive way, the use of age verification may even *encourage* malicious actors to deliberately exploit age verification tools in order to gain access to, and therefore trust within closed spaces. They could do this through the use of cosmetics and prosthetics to trick facial recognition systems (e.g. method 9); by using ID documents belonging to someone else (e.g. methods 5, 6 or 7), perhaps obtained through data breaches, which will inevitably occur more frequently when platforms are required to obtain and store age verification information for their users; or through mimicking behaviours that are associated with children (e.g. methods 10 and 11). Research demonstrating the high risk of identity theft and data fraud was described in Chapter 3, creating yet more risks to people's security online.

Chapter 5: Conclusions

5.1. Centering privacy and safety by design

There is a lack of evidence that age verification measures applied in a widespread way (i.e. for most or all messaging services, social media services, etc.) will be beneficial for children. On the contrary, **document-based age verification** measures rely on the large-scale adoption of a suitable digital identity system. As this paper has explained, the EU will not have this until 2030 (if at all, depending on whether or not the eventual eID wallet is genuinely anonymous and zero-knowledge). Even then, it is likely to exclude 20% of legitimate users. For those without the right documents, such as undocumented young people, no technological developments will prevent their exclusion.

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. Such practices are also likely to amount to profiling and entail a serious risk of discrimination. The legal basis of consent to such profiling, which may need to be invoked by providers under Art. 22 of the GDPR, is unlikely to be lawful in this coercive context.

Some providers are experimenting with combining **document-based age verification and age estimation measures** to offer a choice to users. However, this 'choice' is likely to be illusory, as both document-based age verification and age estimation come with a wide range of risks already discussed. For example, both of these measures still allow providers to set the parameters of what children are able to see online. In addition, they risk locking children out of certain content, or making them feel guilty or fearful to access it (e.g. health or LGBTQI+ content).

The premise that online safety issues can be solved by layering multiple measures also obfuscates the reality that age verification measures can create a false sense of security. In fact, privacy and security by design, as well as appropriate oversight (in line with children's growing autonomy) are likely to be far more effective, as discussed at length throughout this paper. When combined with age **declaration** measures, which are the least risky to children's rights, we find that such measures are most likely to amount to an appropriate balance of children's rights in the digital environment.

More broadly, we have also questioned the premise of requiring formal documents or invasive data processing as a precursor to accessing the digital world, and the limitations on free expression and access to information that this entails. Moreover, we emphasise that in accordance with the Charter, widespread or systematic document-based age verification and age estimation are unlikely to meet the required thresholds of **necessity** and **proportionality**.

A further conclusion that can be drawn from this paper is that age verification should not be considered in the limited frame of technical tools (in particular, document-based age verification and age estimation tools). Instead, age verification should be seen as a spectrum whereby many

non-invasive measures are available, and can be built up cumulatively (including with age declaration measures) to reach a sufficient standard of child protection. In addition to the several safety and privacy by design measures already discussed in this paper, ideas such as content labelling/content warnings, or child versions of services, should be further explored as methods to increase safety in a manner compliant with fundamental rights.

5.2. Recommendations

For lawmakers

1. Given the current lack of effective and rights-compliant tools, as well as the gravity and scale of the risks, **policy- and law-makers must not mandate age assurance** (a term sometimes used as an umbrella for the many different methods), **age estimation or (identity-based) age verification measures** on any general/EU-wide basis;
2. Specifically concerning the EU CSA Regulation, age 'assurance' (the term used in the proposal), verification or estimation measures should not be made mandatory for any providers (Articles 4 and 6), nor should their use be incentivised via the risk assessment and mitigation process (Articles 3 and 4);
3. If optional age verification or estimation measures remain in the CSA Regulation, they must be safeguarded to ensure they meet the thresholds on page 17 and the recommendations in points 8, 9, 12, 13 and 14 below. They should also give providers the ability to meet their obligations through age declaration measures;
4. It is essential that policy- and law-makers, as well as parents and guardians, equip themselves with more information about how age verification tools work, the risks that these tools entail, and the possible alternatives to these intrusive measures;
5. More research could be conducted into rights-compliant age estimation and document-based verification measures, as none of the methods currently available for practical deployment can be regarded as compliant with the rights of the child;[28]
6. The European Commission, Fundamental Rights Agency (FRA) and European Data Protection Board (EDPB) should issue guidelines on age verification in line with the *General Data Protection Regulation*, taking a holistic approach which goes beyond age checks to consider the full spectrum of safety and privacy by design measures;
7. The EU special group on age-appropriate design should develop recommendations for design features and societal measures which will reduce the incentives for young people to falsely declare the wrong age online, thereby increasing the effectiveness of age declaration methods;[29]

For providers of online platforms & services

8. Whenever age verification measures are used, they must be necessary, proportionate, and sufficiently secure; must not allow data to be used for any other purpose; must not retain

[28] This is also the conclusion of the CNIL in the analysis *Online age verification: balancing privacy and the protection of minors* https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

[29] https://zephoria.medium.com/protect-elders-ban-television-2b18ab49988b

data; must not process biometric or biometrics-based data; must never allow the person to be linked to their legal identity or create any sort of profile of them; and must ensure that people can remain fully anonymous online;

9. Any proposed use of age estimation or document-based verification measures must be assessed on a case-by-case basis with the use of a data protection impact assessment (DPIA) and – if the risks are significant – prior consultation with the national Data Protection Authority (DPA);
10. As a general rule, and unless required to do otherwise by national law, providers should use age declaration methods only, until the serious risks and drawbacks of age verification measures have been mitigated, with particular attention to structural exclusion and potential chilling effects;
11. Where document-based age verification measures are proven to be strictly necessary (e.g. for specific use cases at the national level), they should be tightly controlled and steps taken to address all of the risks outlined in this briefing;
12. Based on the assessment here, it seems unlikely that the risks of the age estimation methods discussed can be mitigated enough to make their use acceptable. In particular, the processing of biometric or other sensitive data for this purpose is a red line. However, should future developments show that they can be used in a rights-compliant way, their use should also be tightly controlled and steps taken to address all of the risks outlined in this briefing;
13. When age verification tools are provided by third parties, these third parties must be independent and should not be commercial;
14. As age declaration measures generally have a low-to-medium level of effectiveness, they should be complemented by other measures on a case-by-case basis. This could include changes to content delivery algorithms (recommender systems); ensuring security, safety and privacy by design and by default for all users; content labelling; and by making it less attractive for users to lie about their age;

For all of society

15. We encourage a broader societal debate about the need for and use of age verification measures, including whether age verification tools are the right tools to solve the problems at hand, or if these are social problems requiring structural intervention;
16. We stress that participation in online and offline society should never become contingent on identity documents.;
17. We recommend that parents, teachers, social workers and other educators and persons in positions of authority provide guidance and support to accompany children to relate to and understand the risks of online content, whilst recognising the need for children's agency and privacy.