Children's Rights and Online Age Assurance Systems: The Way Forward

Livingstone, S.; Nair, A.; Stoilova, M.; Hof, S. van der; Caglar, C.

BRILL

THE INTERNATIONAL JOURNAL OF CHILDREN'S RIGHTS
32 (2024) 721–747

brill.com/chil

Children's Rights and Online Age Assurance Systems

The Way Forward

Sonia Livingstone[a]; *Abhilash Nair*[b]; *Mariya Stoilova*[c]; *Simone van der Hof*[d]; *Cansu Caglar*[e]

a) Director, Digital Futures for Children Centre; Professor, Department of Media and Communications, London School of Economics and Political Science (LSE), London, UK | ORCID: 0000-0002-3248-9862
Corresponding author
s.livingstone@lse.ac.uk
b) Associate Professor of Internet Law; Associate Pro-Vice-Chancellor (Business Engagement & Innovation), Faculty of Humanities, Arts and Social Sciences, University of Exeter, Exeter, UK | ORCID: 0000-0002-8268-3030
A.Nair@exeter.ac.uk
c) Postdoctoral Research Officer, London School of Economics and Political Science (LSE), London, UK | ORCID: 0000-0001-9601-7146
m.stoilova@lse.ac.uk
d) Professor of Law and Digital Technologies, Center for Law and Digital Technologies (eLaw), Institute of the Interdisciplinary Study of the Law, Leiden University, Leiden, The Netherlands | ORCID: 0000-0001-7492-7739
s.van.der.hof@law.leidenuniv.nl
e) Teaching Associate, Queen Mary University of London, London, UK
c.caglar@qmul.ac.uk

Published online 24 October 2024

Abstract

Age assurance is a way to prevent children accessing content, products or services that are potentially harmful to them, ranging from gambling services or alcohol or tobacco or, increasingly, certain products and services online. Now that children's lives are mediated by digital technologies, policymakers are deliberating over the legal, technical and practical challenges. These have been little examined from the perspective of children's rights. By combining legal and social research methods,

Published with license by Koninklijke Brill BV | DOI:10.1163/15718182-32030001
 | ISSN: 0927-5568 (print) 1571-8182 (online)

this article examines the legal requirements for age assurance in Europe, assesses compliance by companies and reveals the consequences for family life. In law and practice, we show that age assurance is often ineffective in protecting children from online risk of harm. Further, as currently implemented it risks children's other rights – to non-discrimination, privacy, to be heard, and their civil rights and freedoms, and remedy. We identify promising directions for the use of age assurance in child online protection, focusing on European policy, regulators and civil society actors.

Keywords

age assurance – age verification – age appropriate – children – rights – Europe – law and regulation

1 Introduction

Age restrictions in some form have long existed concerning children's ability to access content, goods and services. For instance, the sale of alcohol or the provision of gambling services to children are restricted under traditional laws. A robust regulatory regime to prevent children's access has also existed for content ranging from the sale of offline pornography to cinema admission (IRIS *plus*, 2012). For the most part, such restrictions have been uncontroversial, building on cultural norms of child socialisation that have evolved over time, with their scope largely confined to the location where the relevant law applies and where the goods or services are distributed and used. However, the advent of widespread internet access operating across borders and jurisdictions has brought about an abrupt change (Reed, 2012; Nair, 2019). Increasingly, global commercial agents and online communities are reshaping norms and practices, disrupting the long-established co-existence of law and local community practices.

This article provides a comprehensive review of the legal, policy and practical considerations surrounding age assurance as it is currently being debated in relation to children's internet use. We take a child rights perspective and focus on the European context, although the challenges and considerations we discuss may also apply elsewhere. Both the European Union and the wider Council of Europe have mainstreamed children's rights frameworks, incorporating the United Nations' Convention on the Rights of the Child (CRC; UN, 1989) in Article 24 of the EU Charter of Fundamental Rights (EU, 2012), the *EU Strategy on the rights of the child* (EC, 2021a), and various aspects of

regulation including in relation to the digital environment; also relevant is the Council of Europe's latest *Strategy for the Rights of the Child* (2022–27) (CoE, 2022). Nonetheless, although in principle, what applies offline also applies online, the regulatory and practical challenges remain considerable, as we discuss.

Although children comprise one in three internet users (Livingstone *et al.*, 2015), and online opportunities for children have been much celebrated, the digital environment is implicitly, if not explicitly, built for adult users and remains poorly designed for children. Children's voices are seldom heard and their needs rarely anticipated when digital products and services are developed (Lenhart and Owens, 2021). One consequence is that children encounter content, contact, conduct and contract risks online (Livingstone and Stoilova, 2021; OECD, 2021), to the dismay of policymakers and the public. While regulators seek to ensure children's online safety, whether by applying offline laws online or developing new laws and regulations (Reed, 2012; Lievens *et al.*, 2018), they face a challenge distinctive to the internet. Unlike when children enter a shop or cinema for age-restricted products, online it is not readily apparent which user is a child (Lessig, 1999). In such circumstances, how can children's experiences be made age appropriate and rights respecting?

Although anonymity has long been the norm online, increasingly users can be identified by age, albeit with variable accuracy. Innovation in data-driven technologies means that considerable information is being collected about users, opening new means of identifying their age. The public, private and third sector actors broadly welcome the burgeoning safety tech market (O'Neill *et al.*, 2020; Billinge *et al.*, 2021; Perspective Economics and DCMS, 2021). This includes various age assurance measures (such as age verification, age estimation and self-declaration) to determine the age or age range of an individual, with varying levels of confidence. These may be required by law or deployed by businesses to suit their intended market. However, their effectiveness in protecting children and meeting other legal requirements is yet to be established (DCMS, 2020; 5Rights Foundation, 2021). A rapid evidence review of families' experiences with age assurance and parental control tools concluded that age assurance is rarely implemented effectively, even at the point of purchase or delivery (Smirnova *et al.*, 2021; see also Nikitin *et al.*, 2016; Gaiha *et al.*, 2020). The International Telecommunication Union (ITU) (2020, p. 9) observed that, 'with surveys showing that most children are using social media before the minimum age of 13 and age assurance services being generally weak or lacking, the risks facing children can be serious.'

As digital technologies become infrastructural for communication, education, health, commerce, work and more, what are the implications for

children's rights of the increasing deployment of age assurance? If certain content, services or products are associated with harmful outcomes for children, it may be legitimate not to give them access. However, the effect on all children's civil and political rights (UN, 1989) – notably, not only protection but also provision, privacy and participation – should be considered holistically. In short, use of age assurance simply to restrict or exclude children from online experiences, rather than as part of a child rights-respecting design and policy, is problematic. Children's evolving capacities (Article 5, CRC) must also be supported, meaning that digital design and policy should be age appropriate within the category of birth to 18. Further, children's rights must be considered in relation to the human rights agenda: crucially, every user may need to undergo age assurance for children to be protected and fairly treated online. This has generated considerable resistance from digital rights groups to age assurance on the grounds of privacy and freedom of expression of adults, as well as from businesses resisting what they see as commercial interference and user friction (see Phippen, 2016; Yar, 2020). Such resistance matters to children for two reasons: privacy and expression are as much rights for children as for adults, and adult resistance may impede the implementation of child protection measures.

In applying a child rights lens to European law, policy and practice regarding age assurance, we draw on and synthesise the insights from three complementary methods. The first was a study of existing laws and regulations relevant to mandatory age assurance applicable to online content, online gambling and the online sale of alcohol and tobacco in the EU and UK (this involved a two prong approach comprising desk-based research and targeted consultations with selected regulators and national experts comprehensively to compile and analyse the relevant laws and regulations across all 27 EU Member States and the UK that apply to online gambling, sale of tobacco and alcohol online and the transposition/implementation of the Audiovisual Media Services Directive 2018; Caglar and Nair, 2021). The second was a review of methods in the EU for obtaining parental consent and maintaining children's rights (the methodology combined desk-based research with a simulation of the user journey of children on websites and in apps from multiple jurisdictions; van der Hof and Ouburg, 2021). The third was a rapid review of the evidence on age assurance and parental control tools from the perspective of children and families. This followed the Preferred Reporting Items for Systematic Review and Meta-Analysis Protocol (PRISMA-P) guidelines to search five major multidisciplinary and subject-specific databases, identifying 1,656 results of which 61 remained for analysis after screening against the review criteria (Smirnova *et al.*, 2021).

In what follows, we first consider the legal requirements for age assurance in Europe. Second, we examine how age assurance tools are currently implemented in practice in light of these requirements. Third, we consider the meanings and practices of age assurance in the everyday lives of children and their families. Fourth, we ask whether age assurance is needed to guarantee children's rights online. Fifth, we examine whether age assurance systems themselves respect children's rights. We conclude with recommendations for age assurance systems that prioritise children's rights.

2 The Legal Requirements for Age Assurance

Legal requirements for age assurance fall into two broad categories – strict legal requirements or risk-based provisions (Shaffique and van der Hof, 2024). Strict legal requirements can explicitly specify the mandatory implementation of age assurance for providers to offer their service, obtain a licence and/or lawfully conduct their business. This is typically the case for gambling services or the online sale of dangerous or unhealthy goods such as tobacco and alcohol. Such laws allow no flexibility for service providers/operators, making it unlawful for them to offer their services to persons under the stipulated age limit. This deliberately sets a high bar by *requiring* age verification, based on making an individual assessment for compliance with the law. Age verification as a subset of age assurance guarantees that the required minimum age is established with a high level of certainty. For example, in the UK, the law criminalises permitting a person under the age of 18 to gamble (section 46, Gambling Act 2005), and the national gambling regulator (Gambling Commission) has issued legal guidelines that mandate age verification. To provide lawfully an online service (e.g., gambling) or sell an age-restricted product (such as alcohol or tobacco), the service provider is required to adopt a high level of age assurance involving age or even identity verification (5Rights Foundation, 2021). There may also be private law requirements that demand age assurance: depending on the applicable law, children may have limited or no capacity to perform legal acts, including concluding a contract. This would make age assurance necessary when, for example, commercial transactions such as in-app or other purchases are included in a digital service.

However, a pan-European study found that there are divergent approaches in the framing and application of the laws across jurisdictions (Caglar and Nair, 2021). Few EU Member States have incorporated laws and policies that specifically address the online sale of age-restricted goods such as alcohol and tobacco. Most jurisdictions assume that established law regarding the sale of

age-restricted products and gambling also apply online, although this is far from guaranteed to be effective. A few countries such as Germany and the Netherlands have found it necessary to introduce specific legal provisions that require age verification mechanisms for the online sale of age-restricted products. In Germany, the legal obligation pertaining to the sale of alcohol and tobacco requires the service provider to implement reliable age verification methods referred to under the guidelines published by the supervisory authority. Additionally, the delivery person is obliged to verify age by requiring the customer's ID as proof. According to the recently amended Alcohol Act in the Netherlands, a seller can lawfully sell alcoholic beverages online only if the appropriate technical measures are implemented at the point of both order and delivery.

Other European laws have been newly incorporated or revised with the advancement of technology. For example, the revised Audiovisual Media Services Directive (AVMSD; EC, 2018), the General Data Protection Regulation (GDPR; EC, 2016) and the Digital Services Act (DSA; EC, 2022) are primary instruments that set particular risk-based obligations on organisations to protect European children specifically from the harmful effects of the digital environment. The GDPR and DSA implicitly require business operators to conduct some form of age assurance to comply with the requirements of the law, while the AVMSD takes a more flexible approach. Under the GDPR, AVMSD and DSA, the level of age assurance to be deployed may depend on the risk involved. Specifically, for age assurance to comply with the GDPR, the chosen method must be proportionate to the nature and risks of the processing activities (Data Protection Commission Ireland, 2021; European Data Protection Board, 2020, nr. 132). Processing the personal data of children is likely to be high risk (van der Hof and Lievens, 2018) and thus demands a high-level age assurance. Similarly, the AVMSD adopts a risk-based approach to determine the mechanisms to be implemented based on various factors such as the risk of harm content may cause, viewers who are intended to be protected and the interest of the relevant stakeholders and the general public (Bakalis and Hornle, 2021).

Accordingly, not all content requires the implementation of robust age assurance methods. Service providers may either choose to distribute content appropriate for all ages or deploy measures taking into consideration the age appropriateness of the content to ensure child viewers are protected from its possible harmful impact (Livingstone and Pothong, 2023). Likewise, the DSA requires providers of online platforms among others to implement *proportionate* measures to ensure a high level of privacy, safety and security of minors (Article 28, DSA), which implies a risk-based approach that may include age assurance if this is an adequate instrument effectively to address risks to children. In addition, the risk-based approach is explicit for what are called very

large online platforms (VLOPs) and very large online search engines (VLOSEs) in the case of systemic risks that include negative effects for the exercise of the rights of the child and for the protection of children (Article 34, DSA). Age assurance, in that case, can be an adequate tool to mediate an age-appropriate experience on these platforms for children and prevent possible harm to their rights and welfare in case of systemic risks.

It has not thus far proved possible to set a uniform standard across Europe as to what constitutes "harmful content", unlike for some illegal content such as child sexual abuse material. Cultural, societal and historical factors influence the acceptability of content in each jurisdiction, with content deemed acceptable for a certain age group in one country being regarded as unacceptable in another. Hence, age assurance methods, if proportionate, would have to cater to different legal requirements across Europe (Caglar and Nair, 2021). The AVMSD stipulates that the most harmful content, such as pornography or gratuitous violence, is subject to the strictest measures (including age verification) (Articles 6(a) and 28b). Member States take a more flexible approach to other types of content, including allowing parents and caregivers (henceforth, parents) and children to make their own decisions on whether viewing content is appropriate, provided they have been clearly informed about the possible harmfulness of content for specific ages, as required by Article 6(a), AVMSD. However, such transparency is not often offered by video platforms hosting user-generated short-form videos, leaving users, including children (often without the parents' knowledge), unexpectedly confronted or personally targeted with unwelcome, inappropriate or undeniably harmful content. In addition, as explored below, lack of clear guidelines from regulators as to how appropriate measures can be implemented in practice could leave both service providers and users with considerable uncertainty.

Regardless of whether age assurance is a strict legal requirement or risk-based, it will usually have to be conducted online when using digital technologies connected to the internet. Exceptions exist in the case of age-restricted products (e.g., alcoholic beverages) if the age can be checked at the point of delivery by means of clear proof of identity. In theory, it is also imaginable that, prior to using certain digital services, someone might first have their age verified online, but such a practice is not yet available. As we discuss in the next section, age assurance is often poorly implemented in digital contexts, using methods that can be easily circumvented by children, thereby exposing them to inappropriate content, harmful products and services, and depriving them of the high level of data protection mandated by the GDPR (van der Hof and Ouburg, 2022). This raises questions about the extent to which existing practical tools satisfy what is required by law, and whether they respect children's

rights by both protecting children from harmful content and services and mitigating the risk of excessive barriers that exclude children from legitimate content and services they are entitled to access. The next section reviews the challenges that arise from how age assurance works in practice.

3 Age Assurance in Practice

Legal requirements for online age assurance, whether strict or risk-based, are not generally supplemented with specifications that such systems must meet, or with guidance on practical implementation (Caglar and Nair, 2021). Consequently, service providers face uncertainty regarding the operational measures required for their age assurance to be legally compliant and child-rights respecting. Some countries provide guidance, for example in Germany ((Kommission für Jugendmedienschutz (KJM), no date), France (CSA, 2011, CNIL, 2022) and Spain (AEPD, 2023), and new standards for age assurance are emerging (5Rights Foundation, 2021; Shaffique and van der Hof, 2024). Compared with other sectors, there is more guidance on age assurance in the gambling sector, where typically age verification alone is not deemed sufficient, and service providers are also required to verify the participant's identity. In Estonia, for example, business operators are recommended to check the age of the participant from the Certification Centre or through an accredited third party such as banks (Maksu- ja Tolliam, 2021). Portugal and Slovakia, for instance, also require the age of the participant to be verified using public registers. However, not all countries have public registers, and across Europe each jurisdiction has its own requirements and circumstances. For instance, in the UK there is no public register, so the business operator must verify the user's age through other options such as credit card verification.

The most common method of age assurance currently used is self-declaration. This is not a reliable method and does not satisfy the strict legal requirements of age verification or the high assurance methods required by the GDPR for the processing of children's personal data (Data Protection Commission Ireland, 2023) and the AVMSD for adult-only content. While it might be appropriate for low-risk situations, it may be supplemented in other ways, for example by capacity testing where the user must solve a task or puzzle that indicates their likely age (van der Hof and Ouburg, 2022). High(er) assurance methods include age verification based on age tokens stored on the user's device and authenticated by third parties with reference to (government) databases have the advantage of not having to maintain a centralised database with large amounts of personal data that is vulnerable to security risks, and being able to

use different data sources in the verification process (Nash *et al.*, 2013; 5Rights Foundation, 2021).

Some age assurance methods provide age *estimation* rather than age *verification* by roughly calculating the age of the user along with the probability of error. One method asks the user to scan their face using a camera so that AI facial analysis trained on a huge volume of images can estimate their age. Other methods include online profiling of users based on their behaviour (van der Maelen, 2018, 2019) or voice recognition. Critics of age estimation methods point out that they do not work equally well with everyone and vary according to gender, age and skin tone (5Rights Foundation, 2021). The reliability of such systems is hard to verify independently or to explain clearly to users, especially children. AI systems for automated recognition, behavioural analytics and biometric systems give rise to considerable concern regarding data privacy and security (5Rights Foundation 2021; Jelinek and Wiewiórowski, 2021; ICO, 2023). Although age assurance systems themselves must comply with the law, including the GPDR and DSA, there is a need for clear guidelines on the security, transparency and inclusiveness of age assurance methods with specific attention to those methods using artificial intelligence. Also potentially problematic is whether such methods lead to a normalisation of surveillance when children (and others) are constantly asked to authenticate with their faces for access to digital services (Burgess, 2021). The effects of age assurance methods should therefore be subject to an evidence-based impact assessment that takes children's rights and wellbeing into account.

Learning from established digital identification technologies deployed in banking or computer security, it may be necessary to join several methods, combining human inputs (e.g., PIN code or password or self-declared age) with technical authentication or trusted third party authentication services. By contrast with such approaches, many current age assurance methods – especially self-declaration – provide far too low a level of age assurance to meet legal obligations. Such tools are also problematic because, although age assurance is the responsibility of digital service providers who must comply with applicable legal requirements (ICO, 2023), they seem to shift the responsibility from digital service providers to children and parents by expecting them to provide the correct age or date of birth at registration. Also problematic is that, when children do use digital services below the minimum age set by providers, they find themselves using services that do not consider their safety specifically and may therefore not be age appropriate (Data Protection Commission Ireland, 2023).

The lack of practical guidance on age assurance combined with rapid innovation by age assurance providers makes it hard to establish how such methods affect the rights of users, including children. Some methods that may seem

technically suitable for age assurance might, in practice, interfere with children's rights in ways that are not self-evident. For instance, online age verification using hard identifiers, such as an ID card, are not meant for online verification and can reveal more personal data than necessary for verifying simply whether someone has reached the minimum age required by law (5Rights Foundation, 2021). Moreover, such hard identifiers are considered disproportionate by the Irish Data Protection Commission given that children may not have access to them, and such a requirement may disproportionately affect children from minority backgrounds (Data Protection Commission Ireland, 2023). Indeed, using credit cards for age verification may not only exclude children altogether but also some adults who are not eligible to obtain credit cards, for instance due to poor creditworthiness. From a child rights perspective, critical attention should also be paid to the specific age restrictions set by providers. Some may represent a genuinely informed assessment of children's best interests (Article 3, CRC) and evolving capacities (Article 5, CRC). But most represent a business decision to exclude children rather than invest in designing services appropriate for them. Such a business decision becomes cynical if children's exclusion is then poorly managed through use of weak age assurance measures, while digital providers continue to profit from children's engagement and children continue to be placed at risk (Livingstone *et al.*, 2024).

4 Age Assurance in the Lives of Children and Families

As with the adoption of most domestic technologies, the mundane practices of everyday life are critical to the success of child protection measures. Given families' diversity of composition, values, practices, digital skills and circumstances, it is hardly to be expected that age assurance will bring about the same outcomes across households. Indeed, research on the "domestication" or "appropriation" of technologies reveals an active process of meaning-making heavily shaped by the structures and activities of everyday life (Hartmann, 2023; Chambers, 2016). Once embedded within the home, the meanings and potential of technologies evolve in accordance with the dynamics of everyday life, the practices and imaginaries that surround their use and the choices that families make. We can therefore expect age assurance technologies to become associated with a range of meanings and practices beyond those anticipated by law or business, including partial use, or misuse, or creative workarounds. For example, children may borrow parents' IDs (Williams *et al.*, 2018) or obtain gift cards (van Hoof, 2016) to purchase age-restricted goods, or simply provide a wrong age in the case of self-declaration (DRCF, 2022). Since parents often

believe they should have the final say about what is age appropriate for their children, they may even help them to "break the rules" (Revealing Reality, 2021). On the other hand, a UK survey found that as children approach the so-called "digital age of consent", parents appear more worried, preferring a still-older age (Livingstone and Ólafsson, 2018).

The everyday implementation of age assurance poses internet users with occasional or frequent decisions both about access to certain content, services or products online, and about whether to provide the personal information needed to establish their age. Yet, by comparison with the very sizeable literature on parental rules and mediation of children's internet use (Elsaesser *et al.*, 2017), little research has asked how age assurance is managed in the domestic context. Consider, for example, the situation for children with disabilities or refugees who lack government IDs, or those whose parents are in conflict about their digital activities. Since children's needs and capacities are not universal, "catch-all" measures might precisely leave out those groups of children who are already more disadvantaged and who would benefit most from digital inclusion. Indeed, to the extent that policymakers rely on parental management of children's digital activities, the outcomes will likely be iniquitous given parents' differential resources, expertise and competence to manage and mediate the impact of the digital environment on their child. Unfortunately, little evidence is available on the use of age assurance across diverse family forms or vulnerable groups, impeding conclusions about the feared consequences for inequality and exclusion, potentially affecting children's right to non-discrimination (Article 2, CRC), as well as the realisation of their other rights (to protection, information, privacy and expression) in a digital world.

The pan-European EU Kids Online survey explored parental attitudes to the future possibility of requiring parental permission for children under 16 to use social media, apps and smart devices (Smahel *et al.*, 2020). Depending on the country, between one- and two-thirds of parents were unsure how such measures could work, up to half did not understand why such permission might be necessary or would find it difficult to decide, and between a third and two-thirds did not feel it would make much difference to how their child uses apps or services. Moreover, between one-fifth and two-fifths thought such a measure would harm their child's privacy from their parents or limit their agency to make their own decisions. However, most parents saw such measures as helping them stay more in control and keeping their child safer online, even though they worried that it could make it harder for their child to stay in touch with their friends. The findings also showed that parents' views about their children becoming independent online vary substantially between countries (for example, they appear more relaxed in Poland and Norway than in Germany or Spain

about their child making their own decisions regarding their digital activities; Smahel *et al.*, 2020).

Relatedly, a recent review of studies of parental mediation strategies found that what matters to children's experience of online risk is the warmth of the child–parent relationship and the collaborative and communicative actions this enables, more than any use of technical tools, surveillance or restrictions (Elsaesser *et al.*, 2017). And although such tools are often advertised as "controls", many parents seek ways to integrate them as part of positive parenting, including for co-use or joint media engagement (Ewin *et al.*, 2021). Meanwhile, more restrictive or controlling approaches can result in children evading or conflicting with parental decisions (Third *et al.*, 2019; Livingstone and Blum-Ross, 2020). Moreover, with parental consent and age assurance increasingly embedded in parental control tools (Stoilova *et al.*, 2023), it can be hard for parents, policymakers and child rights advocates to know which data are being collected and how these affect children's access to digital services.

Age assurance and other forms of access regulation, whether managed by the state or businesses, could in principle ease the task parents face in bringing up their children in a rapidly innovating digital environment. However, it is not currently evident whether the growing complexity of digital regulation is beneficial for children overall, including whether age assurance can be designed in ways that respects children's rights holistically without stimulating new and creative workarounds. Furthermore, it is not yet clear that the design and operation of age assurance technology itself facilitates rather than infringes children's rights.

5. Age Assurance as a Means to Guarantee Children's Rights

To safeguard children's rights in the digital environment, it is necessary to know when users are likely to be children, unless digital services are made appropriate for all ages by design. Even general-purpose sites such as Google Maps, Wikipedia, Chess.com or Amazon give pause for thought: maps may publicise users' location; online encyclopaedias may contain misinformation; gaming sites may enable chat between adult and child players; online shopping sites may sell knives and alcohol; and any of these may use children's personal data for commercial purposes in ways that are not privacy-preserving or even lawful. For the most part, age assurance has been deployed to protect children from online content, products or services that are unlawful or harmful for them to use, to preserve their safety and privacy and to comply with contract law.

Although the CRC does not contain an obligation of age verification, it may be deemed necessary, as recognised by the UN Committee on the Rights of the Child in its General Comment No. 25: 'Robust age verification systems should be used to prevent children from acquiring access to products and services that are unlawful for them to own or use' (UN, 2021, para. 114). "Robust" sets the expectation that age verification systems should be used if they are effective in keeping very high-risk harms away from children, implicitly setting a threshold that, in practice, many systems do not meet. Beyond such unlawful risks, another reason for using age assurance can be found in Article 17 of the CRC that 'encourage[s] the development of appropriate guidelines for the protection of the child from information and material injurious to [their] well-being'. Keeping harmful content, services and products away from children is arguably also necessary to ensure the best interests of the child (Article 3, CRC), to take account of their evolving capacities (Article 5, CRC) and support the fullest development of children (Articles 6 and 29, CRC).

However, it is important that content, services and products are not arbitrarily kept from children as this may interfere with their other rights, including the right to freedom of expression and information (Article 13, CRC), association (Article 15, CRC) and privacy (Article 16, CRC). Digital services can make a hugely important contribution to children's development and should therefore be accessible to children – consider the provision to children of information about sexuality and sexual health (Livingstone and Mason, 2015). The threshold for age-based restrictions should be set according to whether, on balance, content, services or products are potentially harmful to children or certain age groups of children, bearing in mind all their rights. Should evidence regarding the harmful nature of content or services be lacking, the precautionary principle may apply. This entails a "better safe than sorry" approach where regulators should ban certain practices (e.g., online profiling of children for commercial purposes), and providers would be legally obliged to mitigate the potentially negative impact on the rights and wellbeing of children's (Lievens, 2021). For example, the rationale for traditional regulation of adult pornography, which imposes legal obligations on publishers and distributors to restrict children's access, has relied on perceived risks of harm rather than conclusive clinical evidence of harm resulting from exposure (Nair, 2019). Note that this may not necessarily imply an obligation to verify age; some decisions can be left to the discretion of parents (in line with Article 18, CRC) or children themselves, providing they are clearly informed about the ages for which the content may be harmful and why. As General Comment No. 25 sets out (UN, 2021), and as reflected in the EU's AVMSD, in addition to or instead of age assurance, alternative measures include content labelling, content moderation, filtering systems,

reporting mechanisms and provision of positive content; what matters is that, in a given context, it must be established which measure is proportionate.

Age assurance may also be necessary to ensure that children enjoy a high level of data protection, given that the Committee on the Rights of the Child (UN, 2021) recognised that Article 16 of the CRC encompasses the child's right to data protection and that data protection laws increasingly provide a high level of protection for children's privacy online across interpersonal, institutional and commercial contexts (Stoilova *et al.*, 2020). Again, care is needed to ensure that a high level of data protection does not lead to children being excluded from digital services, given that this may interfere with their other rights. While it might be easier for digital providers to restrict access for all children or younger groups, children should not be deprived of a rich user experience or be offered inferior digital services, supposedly because of data protection considerations. Rather, digital service providers should provide age appropriate privacy-by-design services that respect children's rights (Data Protection Commission Ireland, 2021; Crepax *et al,* 2022; Hsu, van der Hof, 2023). Efforts to provide guidance on what age-appropriate design might entail started in the UK (ICO, 2020) and are now being taken up in other countries such as Sweden, the Netherlands and Turkey, as well as put forward in age-appropriate design standards (IEEE, 2021; CEN and CENELEC, 2023).

Finally, digital services may involve commercial practices that may interfere with the child's right to protection from economic exploitation (Article 32, CRC) and to free play (Article 31, CRC) (van der Hof *et al.*, 2022). Behavioural design that influences children subconsciously to make choices they would not have made otherwise, i.e. deceptive design or dark patterns (Zagal *et al.*, 2013), are likely to be unfair commercial practices under consumer law (Leiser and Caruana, 2021). In addition, children's personal data should not be processed for online targeted advertising because this is a commercial practice that children do not or insufficiently understand and is not in their best interests (van der Hof, Lievens and Milkaite, 2022). Although the UN Committee on the Rights of the Child (UN, 2021) does not explicitly refer to these consumer law-related risks or link them to Article 32 of the CRC, it does recognise that the design of commercial services can be harmful or unfair to children.

6 Designing Age Assurance that Respects Children's Rights

Not only is it important that, insofar as age assurance is advocated to help realise children's rights, it is effective in this regard, but also age assurance tools should themselves respect children's rights. Yet the design and operation of

any technology may facilitate or interfere with a range of children's rights. Attracting most concern in the case of age assurance is the right to privacy. Age assurance systems can operate anonymously – for example, by using an age token on a smartphone (Corby, 2022; Allen *et al.*, 2023), but such decentralised systems are not widely available. Having said that, both the French and Spanish data protection authorities have published guidance on privacy-friendly age assurance (CNIL, 2022; AEDP, 2023). To identify who is (or is not) a child, personal information is generally required, and some methods may be particularly privacy-invasive, such as those based on biometrics and behavioural analytics. Who obtains this data, how it is used and the conditions that regulate this are crucial questions the answers to which may not be immediately apparent to users of digital technologies, including children. In the digital environment, privacy is largely, although not only, regulated as a matter of data protection (applicable when data relates to an identified or identifiable individual).

More and more countries now have data protection legislation (CNIL, 2023), often requiring a higher level of protection for children, although compliance is variable and enforcement by regulators is often weak (van der Hof and Ouburg, 2021). For example, in Europe (and influential beyond Europe), the GDPR requires that data processing must be fair (Article 5, GDPR), lawful (Articles 5 and 6, GDPR) and transparent (Articles 5 and 12, GDPR). Only data necessary for age assurance may be processed by age assurance technologies (Article 5, GDPR: purpose specification and data minimisation). Further, transparency must be age appropriate, meaning that it must be clear to children which of their personal data are being processed and why. Equally, exercising data access rights must be straightforward for children and parents. Where age verification systems use biometrics or profiling, they must comply with stricter requirements (Articles 9 and 22, GDPR). In the EU, the AVMSD specifically prohibits commercial uses of personal data processed for age assurance purposes (Article 6a (2), AVMSD; see also General Comment No. 25 (UN, 2021, para. 77)). Similarly, the DSA stipulates high levels of privacy and safety for children, recognising that this may require age assurance; it further stipulates that this should not require providers of online platforms to process additional personal data to assess whether a user is a child (Article 28 (3), DSA). Although the meaning of this latter part is not entirely clear, it is likely to be a reference to privacy-friendly age assurance systems (see also Articles 5 and 25, GDPR on data minimisation and privacy by design). Finally, the development of large, centralised databases containing personal data poses information security risks that must be prevented through strong regulation and security-by-design

(Article 32, GDPR; Article 21, NIS2 Directive; see also proposed EU Cyber Resilience Act).

Also of concern is the principle of non-discrimination (Article 2, CRC). Age assurance systems must not discriminate against particular groups of children, notably by unjustifiably excluding them from accessing digital contents, services or products. This can occur if, for example, methods presume access to a credit card or a digital identity tool. Age assurance methods should also avoid using technologies that are potentially biased towards or against certain groups of children and/or their parents or give a high probability of false results, for example by not working well with specific personal characteristics, such as skin tone, ethnicity, gender, disability or age (5Rights Foundation, 2021). Furthermore, developers of age assurance systems should consider children (and adults) with disabilities by providing inclusive (accessible) design, since these users should not face additional barriers because of the use of technology; indeed, existing barriers relating to the digital environment should be removed (Lundy *et al.*, 2019; Hsu and van der Hof, 2023). Children's personal evolving capacities or disabilities or other circumstances should not be a reason to give certain groups of children a less good experience, and user testing is important to ensure that the design of such systems works fairly for everyone.

Children's right to be heard (Article 12, CRC) means that they should be meaningfully involved in the design and development of assurance and consent mechanisms insofar as these impact on their digital lives. Particularly, children must be consulted on the age-appropriate nature of digital services and any age gating for the purposes of their protection, including how choices made in the design of age assurance mechanisms may impact on their (other) rights and best interests (Livingstone *et al.*, 2024). To the best of our knowledge, children have not been formally consulted about age assurance. The process of preparing General Comment No. 25 involved a global consultation with children living in diverse contexts, with special efforts made to consult those living in disadvantaged or marginalised situations. The children consulted were clear in their message to policymakers that accessing the digital environment is no longer optional, but a necessity for their education, information, family life, social relationships, work, identity, play and more (5Rights Foundation, 2021). While they recognised that adults may know more about the risks of the digital world, they were concerned about adult approaches that appear to disrespect their perspectives or fail to hear and take account of their views, claiming that this in itself can lead to adverse outcomes.

A small European study interviewed children and parents, finding that they are broadly positive about age assurance in principle, being familiar with offline precedents (e.g., for purchasing alcohol or accessing pornography)

and in agreement with the need to keep potentially harmful online content, services and products from children (Revealing Reality, 2021, 2023). However, they expressed concerns about age assurance in practice, wishing for flexibility to suit children's interests and maturity as well as parental and community values. Such findings are supported by a UK-based qualitative study with children and parents regarding their attitudes to age assurance (DRCF, 2022). Consulting children, and potentially their parents, makes it clear that methods of child online protection are unacceptable if they simply or high-handedly restrict children's access to the internet without recognising how this may infringe their rights. Still needed are efforts to address children's and parents' scepticism that the existing guidance, age ratings, labelling or certification match children's needs and development. Provisions are often taken only as guidance, and parents sometimes feel that they need to override mechanisms that curtail their children's access to the digital environment. Indeed, purely restrictive measures can even result in children seeking to bypass them, while parents may be reluctant to concede their authority to systems that are not flexible enough to meet their children's needs as they see it (DRCF, 2022).

Finally, children must be provided with easy access to effective and child-friendly instruments to enable them to make complaints when their rights are not observed or get support in using age assurance (Council of Europe, 2012; Lievens *et al.*, 2018; ICO, 2020). This, and the foregoing problems, can be addressed by expecting or even mandating use of a children's rights impact assessment (UN, 2013; UNICEF/The Danish Institute for Human Rights, 2013; Mukherjee *et al.*, 2021). In this way, it is possible to assess holistically the positive and negative impacts on children's rights of a decision or policy such as age assurance, and to determine what (age-) appropriate safeguards need to be implemented. Here, too, it is important to consult children to gain insight into the obstacles they experience when using or being subject to such methods so as to design age assurance systems that are child friendly and age appropriate.

7 Conclusions

There is now growing recognition of the need for age assurance online, with recent legislative initiatives in different parts of the world including Europe, Australia, India and the USA calling for age assurance methods for child online protection. The UN's specialist technology agency urges that businesses should, 'where possible, use age assurance to limit access to content or material that, either by law or policy, is intended only for persons above a certain age' (ITU, 2020: 32), adding that it is essential, 'that age assurance systems do

not jeopardise the genuine need for specific age groups to access content that is relevant for their development' (26) nor 'endanger their privacy' (32). As we have shown, although various laws in the EU have long envisaged age assurance to protect children from harmful content, products and services online, the enforcement of such laws has been ineffective, with a few exceptions such as online gambling. As illustrated by the spectacular failure of laws designed to prevent children's access to adult pornography (Nair, 2019), laws that are not enforced will not command the respect or obedience of those who are bound by them, and will ultimately fail (Reed, 2012).

Meaningful implementation of laws that require age assurance, whether "hard" age and identity verification or a "softer" age estimation, necessitate effective age assurance methods being in place. Notwithstanding child rights and wider societal concerns and resistance to age assurance, it is highly likely that such tools will be increasingly used across the digital environment. For this reason, it is important to get it right. Writing for the International Engineering Standards Association, Pasquale *et al.* (2020: 7) 'recommend age assurance as an ongoing process that does not terminate after sign-up' together with efforts to incentivise honesty, not deception, by users about their age. Even if this is developed, it is fair to conclude that 'age assurance should not be mistaken for a silver bullet or a shortcut to making the digital world fit for children' (5Rights Foundation, 2021: 4), there being a need for 'a mixed economy of age assurance methods' (7); a child rights approach would hope, further, that –

> rather than being the route to keeping children out of the digital world, age assurance can drive the development of new products and services to create a richer and more diverse digital ecosystem in which children (one in three internet users) are a recognised user group (9).

In the search for robust, rights-respecting systems of age assurance for the online protection of children, the task ahead is considerable, since the nature of the digital environment continually evolves, posing new challenges to children's rights, including their safety and privacy. There are, crucially, gaps and slippages between policy frameworks, policymaking and policy implementation, with EU member states struggling at times to keep pace with socio-technological developments or to enact sufficient multistakeholder cooperation for a smooth transition from policy frameworks to full and effective implementation on a national basis (O'Neill *et al.*, 2023). Reporting on progress, O'Neill *et al.* (2023) observe an increase in implementation of EU legislation with three-quarters of European countries taking steps to implement age-appropriate privacy settings, in accordance with the GDPR, and 83 per cent with also

promoting the adoption of age rating and content classification as required by the AVMSD. However, although age assurance "solutions" of different kinds are actively being developed, a European review concluded that, 'while there is a clear need for protecting children online, there are currently no age assurance methods that adequately protect individuals' fundamental rights' (Sas and Mühlberg, 2024: 7).

Although age assurance remains controversial, there remain strong grounds for age assurance as a norm, together with privacy and safety-by-design, to provide children with age-appropriate digital opportunities as well as protections. To ensure such measures are effective and proportionate (FOSI, 2023), respecting the full range of children's rights, a range of child rights approaches can be useful, including robust evaluations, child consultation and participatory design. Indeed, including age assurance methods in the child rights impact assessment of digital services subject to legal age assurance requirements (Mukherjee *et al.*, 2021) would be an effective way of ensuring that these methods are inclusive, effective and responsive to technological and regulatory innovation (Data Protection Commission Ireland, 2021; European Data Protection Board, 2020, nr. 146; Data Protection Commission Ireland, 2023). However, child rights approaches are currently insufficiently familiar to digital providers and internet governance policymakers.

Commercial innovation, regulatory frameworks and societal expectations are co-evolving, resulting in a digital environment that requires considerable intervention if it is sufficiently to respect children's rights (Third *et al.*, 2019). Some of these interventions are broadly effective and trusted by the public, even taken for granted as part of modern life in a civilised society. Some are little used or not trusted, already known for their failings and available workarounds. Yet others are contested for protecting children at the cost of their civil rights and freedoms or for professing to protect children at the cost of adult freedoms in a digital world. Thus far, age assurance is only partially trusted and subject to contestation, though this might be improved by setting standards for the efficacy of age assurance and age restrictions, combined with certification schemes as a statutory requirement for providing age-restricted content. Further, the impact on child users and children's rights has not received due consideration, and we have identified serious concerns regarding protection, discrimination, privacy, the right to be heard, civil rights and freedoms and remedy. Yet, to keep children safe online, age assurance is increasingly mandated by legislation and called for by policymakers and the public. Our analysis of the inadequacies and inconsistencies of age assurance methods demonstrates that both law and practice need further work to respect children's rights. As things stand, there are pressing challenges on both counts.

More positively, it is plausible that age assurance could be designed in ways that respects children's rights, thereby helping to realise children's rights more broadly in a digital world. This article has identified both the promise and the challenges, providing a road map for future work.

Acknowledgements

This research was funded by a grant from the European Commission: PPPA-AGEVER-01-2020 (project number LC-01622116/101018061). We would like to thank our colleagues from the euCONSENT project and the experts who advised us on our work.

References

5Rights Foundation, *But How Do They Know It Is a Child? Age Assurance in the Digital World* (London: 5Rights Foundation, October 2021). https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf.

AEPD (Agencia Española Protección Datos (Spanish Data Protection Agency)), *Decálogo de principios. Verificación de edad y protección de personas menores de edad ante contenidos inadecuados* (*Decalogue of principles. Age verification and protection of minors from inappropriate content*). https://www.aepd.es/guias/decalogo-principios-verificacion-edad-proteccion-menores.pdf.

Allen, T., Mccoll, L., Walters, K. and Lyon, M., *Measurement of Age Assurance Technologies* (Digital Regulation Cooperation Forum, 2023). www.drcf.org.uk/publications/papers/measurement-of-age-assurance-technologies.

Bakalis, C. and Hornle, J., "The Role of Social Media Companies in the Regulation of Online Hate Speech", in A. Sarat (ed.), *Studies in Law, Politics, and Society* (vol. 85) (Bingley: Emerald Publishing Limited, 2021).

Billinge, G., Burgess, R. and Corby, I., *EU Methods for Audiovisual Media Services Directive* (*AVMSD*) *and General Data Protection Regulation* (*GDPR*) *Compliance* (London: The Age Verification Providers Association, 2021). https://euconsent.eu/project-deliverables/.

Burgess, M., "This AI Predicts How Old Children Are. Can It Keep Them Safe?", *Wired* 26 October 2021. www.wired.com/story/ai-predicts-how-old-children-are.

Caglar, C. and Nair, A., *EU Member State Legal Framework* (Birmingham: Aston University, 2021). https://euconsent.eu/download/eu-member-state-legal-framework.

CEN (European Committee for Standardization) and CENELEC (European Committee for Electrotechnical Standardization), "Age Appropriate Digital Services Framework" (September 2023). www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016_2023.pdf.

Chambers, D., *Changing Media, Homes and Households: Cultures, Technologies and Meanings* (Abingdon: Routledge, 2016).

CNIL (Commission nationale de l'informatique et des libertés (National Commission on Informatics and Liberty)), *Online age verification: balancing privacy and the protection of minors*, 2022. https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.

CNIL (Commission nationale de l'informatique et des libertés (National Commission on Informatics and Liberty)), "Data Protection Around the World", 2023. www.cnil.fr/en/data-protection-around-the-world.

Corby, I., "A Summary of the Achievements and Lessons Learned of the euCONSENT Project and What Comes Next", 7 December 2022. https://euconsent.eu/a-summary-of-the-achievements-and-lessons-learned-of-the-euconsent-project-and-what-comes-next.

Council of Europe, *Council of Europe Recommendation on the Participation of Children and Young People Under the Age of 18* (Strasbourg: Council of Europe, 2012). https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680046c478.

Crepax, T., Muntes-Molero, V., Martinez, J., Ruiz, A., "Information Technologies Exposing Children to Privacy Risks: Domains and Children-Specific Technical Controls", *Computer Standards and Interfaces* 2022 (82), 103624. DOI: 10.1016/j.csi.2022.103624.

CSA (Conseil supérieur de l'audiovisuel (Superior Audiovisual Council]), "Délibération du 20 décembre 2011 Relative à la Protection du Jeune Public, à la Déontologie et à l'Accessibilité des Programmes sur les Services de Médias Audiovisuels à la Demande", 30 December 2011. www.csa.fr/Reguler/Espace-juridique/Les-textes-reglementaires-du-CSA/Les-deliberations-et-recommandations-du-CSA/Recommandations-et-deliberations-du-CSA-relatives-a-la-protection-des-mineurs/Deliberation-du-20-decembre-2011-relative-a-la-protection-du-jeune-public-a-la-deontologie-et-a-l-accessibilite-des-programmes-sur-les-services-de-medias-audiovisuels-a-la-demande.

Data Protection Commission Ireland, *Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing*. Final Version, December 2021 (Dublin: Data Protection Commission, 2021). https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf.

Data Protection Commission Ireland, *Decision in the matter of TikTok Technology Limited made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation*. https://www.edpb.europa.eu/system/files/2023-09/final_decision_tiktok_in-21-9-1_-_redacted_8_september_2023.pdf.

DCMS (Department for Digital, Culture, Media & Sport), *VoCO* (*Verification of Children Online*): *Phase 2 Report* (London: Home Office, November 2020). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/934131/November_VoCO_report_V4__pdf.pdf.

DRCF (Digital Regulation Cooperation Forum), *Families' Attitudes Towards Age Assurance: Research Commissioned by the ICO and Ofcom* (DRCF, 11 October 2022). www.gov.uk/government/publications/families-attitudes-towards-age-assurance-research-commissioned-by-the-ico-and-ofcom.

Elsaesser, C., Russell, B., McCauley, C. and Ohannessian, D. P., "Parenting in a Digital Age: A Review of Parents' Role in Preventing Adolescent Cyberbullying", *Aggression and Violent Behavior* 2017 (35), 62–72. DOI: 10.1016/j.avb.2017.06.004.

European Commission (EC), Digital Services Act, *Official Journal of the European Union*, 2022: 277, 27.10.2022. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.

European Data Protection Board, *Guidelines 05/2020 on Consent under Regulation 2016/679* (Brussels: European Data Protection Board, 4 May 2020). https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

European Parliament and the Council of the European Union, *Regulation* (*EU*) *2016/697 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*) (Offical Journal of the European Union, 4 May 2016). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

European Parliament and the Council of the European Union, *Directive* (*EU*) *2018/1808 of the European Parliament and of the Council of 14 November 2018 Amending Directive 2010/13/EU 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*) *in View of Changing Market Realities* (Official Journal of the European Union, 28 November 2018). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1808.

Ewin, C. A., Reupert, A. E., McLean, L. A. and Ewin, C. J., "The Impact of Joint Media Engagement on Parent–Child Interactions: A Systematic Review", *Human Behaviour and Emerging Technologies* 2021 (3(2)), 230–254. DOI: 10.1002/hbe2.203.

FOSI (Family Online Safety Institute), *Coming to Terms with Age Assurance* (Washington, DC: FOSI, July 2023). https://global-uploads.webflow.

com/5f4dd3623430990e705ccbba/64b0011a158eea37fb7796c4_FOSI%20White%20Paper%20Coming%20to%20Terms%20with%20Age%20Assurance%20FOR%20WEBSITE.pdf.

Gaiha, S. M., Lempert, L. K. and Halpern-Felsher, B., "Underage Youth and Young Adult e-Cigarette Use and Access Before and During the Coronavirus Disease 2019 Pandemic", *JAMA Network Open* 2020 (3(12)), 16. DOI: 10.1001/jamanetworkopen.2020.27572.

Hartmann, M. (ed.) *The Routledge Handbook of Media and Technology Domestication* (Routledge, 2023).

Hsu, L.-R. and van der Hof, S., "Designing Inclusive Privacy for Children – Approaches for Data Protection by Design Protecting and Empowering Children with Intellectual Disabilities", *European Journal of Law and Technology* 2023 (14(3)). https://www.ejlt.org/index.php/ejlt/article/view/939.

ICO, "The ICO's Response to the Call for Evidence and Roundtables on Age Assurance", 2023. https://ico.org.uk/media/about-the-ico/consultations/4023848/20221221-response-to-aa-cfe-and-roundtables-v1_0.pdf.

ICO (Information Commissioner's Office), *Age Appropriate Design: A Code of Practice for Online Services* (Wilmslow: ICO, 2 September 2020). https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf.

ICO (Information Commissioner's Office), TikTok Information Technologies UK Limited and TikTok Inc (TikTok) monetary penalty notice, 2023. https://ico.org.uk/action-weve-taken/enforcement/tiktok/.

IEEE (Institute of Electrical and Electronics Engineers), *2089-2021 – IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children* (New York: IEEE, 30 November 2021). https://ieeexplore.ieee.org/document/9627644.

IRIS *plus*, "Protection of Minors and Audiovisual Content On-Demand" (Strasbourg: European Audiovisual Observatory, 2012). https://rm.coe.int/1680783db7.

ITU (International Telecommunication Union), *Guidelines for Industry on Child Online Protection* (Geneva: ITU Publications, 2020). www.itu-cop-guidelines.com/industry.

Jelinek, A. and Wiewiórowski, W. R., *Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence* (*Artificial Intelligence Act*) (Brussels: European Data Protection Board; European Data Protection Supervisor, 18 June 2021). https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

KJM (Kommission für Jugendmedienschutz) (Commission for the Protection of Minors in the Media), date not available. www.kjm-online.de/en.

Leiser, M. R. and Caruana, M., "Dark Patterns: Light to Be Found in Europe's Consumer Protection Regime", *Journal of European Consumer And Market Law* 2021

(10(6)), 237–251. https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/10.6/EuCML2021047.

Lenhart, A. and Owens, K., "The Unseen Teen: The Challenges of Building Healthy Tech for Young People", *Data & Society* 2021. https://datasociety.net/wp-content/uploads/2021/05/The-Unseen-Teen-.pdf.

Lessig, L., "The Law of the Horse, What Cyberlaw Might Teach", *Harvard Law Review*, 1999 (113), 501–546.

Lievens, E., "Growing Up with Digital Technologies: How the Precautionary Principle Might Contribute to Addressing Potential Serious Harm to Children's Rights", *Nordic Journal of Human Rights* 2021 (39(2)), 128–145. DOI: 10.1080/18918131.2021.1992951.

Livingstone, S. and Blum-Ross, A., *Parenting for a Digital Future: How Hopes and Fears about Technology Shape Children's Lives* (New York: Oxford University Press, 2020).

Livingstone, S. and Mason, J., *Sexual Rights and Sexual Risks Among Youth Online: A Review of Existing Knowledge Regarding Children and Young People's Developing Sexuality in Relation to New Media Environments* (Rome: eNASCO, September 2015). www.lse.ac.uk/business/consulting/assets/documents/sexual-rights-and-sexual-risks-among-youth-online.pdf.

Livingstone, S. and Ólafsson, K., *When Do Parents Think Their Child Is Ready to Use the Internet Independently? Parenting for a Digital Future: Survey Report 2* (London: London School of Economics and Political Science, 2018). http://eprints.lse.ac.uk/87953.

Livingstone, S. and Pothong, K., *Child Rights by Design: Guidance for Innovators of Digital Products and Services Used by Children* (London: Digital Futures Commission and 5Rights Foundation, March 2023). https://eprints.lse.ac.uk/119724/.

Livingstone, S., and Stoilova, M. *The 4Cs: Classifying Online Risk to Children*. CO:RE Short Report Series on Key Topics. (Hamburg: Leibniz-Institut für Medienforschung, Hans-Bredow-Institut (HBI), CO:RE – Children Online: Research and Evidence, 2021): DOI: 10.21241/ssoar.71817.

Livingstone, S., Carr, J. and Byrne, J., *One in Three: Internet Governance and Children's Rights* (Ontario and London: Centre for International Governance Innovation and the Royal Institute of International Affairs, 2015). www.cigionline.org/static/documents/no22_2.pdf.

Livingstone, S., Cantwell, N., Özkul, D., Shekhawat, G., and Kidron, B., *The Best Interests of the Child in the Digital Environment* (Digital Futures for Children Centre, LSE and 5Rights Foundation 2024). https://eprints.lse.ac.uk/122492/.

Lundy, L., Byrne, B., Templeton, M. and Lansdown, G., *Two Clicks Forward and One Click Back: Report on Children with Disabilities in the Digital Environment* (Strasbourg: Council of Europe, 2019). https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f.

Maksu- ja Tolliamet (Tax and Customs Board), *Organisation of Remote Gambling* (Tallinn: Maksu- ja Tolliamet 2021). www.emta.ee/eng/organisation-remote-gambling.

Mukherjee, S., Pothong, K. and Livingstone, S., *Child Rights Impact Assessment: A Tool to Realise Children's Rights in the Digital Environment* (London: Digital Futures Commission, 5Rights Foundation, March 2021). https://eprints.lse.ac.uk/119727/.

Nair, A., *The Regulation of Internet Pornography: Issues and Challenges* (Abingdon: Routledge, 2019).

Nash, V., O'Connell, R., Zevenbergen, B. and Mishkin, A., *Effective Age Verification Techniques: Lessons to Be Learnt from the Online Gambling Industry* (Oxford: Oxford Internet Institute, 2013). www.oii.ox.ac.uk/archive/downloads/publications/Effective-Age-Verification-Techniques.pdf.

Nikitin, D., Timberlake, D. S. and Williams, R. S., "Is the E-Liquid Industry Regulating Itself? A Look at E-Liquid Internet Vendors in the United States", *Nicotine & Tobacco Research* 2016 (18(10)), 1967–1972. DOI: 10.1093/ntr/ntw091.

O'Neill, B., Dreyer, S. and Dinh, T., *The Third Better Internet for Kids Policy Map: Implementing the European Strategy for a Better Internet for Children in European Member States* (Brussels: European Schoolnet, 2023). https://www.betterinternetforkids.eu/policy/bikmap.

OECD (Organisation for Economic Co-operation and Development), *Children in the Digital Environment – Revised Typology of Risks* (Paris: OECD, 2021). www.oecd-ilibrary.org/content/paper/9b8f222e-en.

Pasquale, L., Zippo, P., Curley, C., O'Neill, B. and Mongiello, M., *Digital Age of Consent and Age Assurance: Can They Protect Children?* (New York: IEEE, 2020). DOI: 10.1109/MS.2020.3044872.

Perspective Economics and DCMS (Department for Digital, Culture, Media & Sport), *The UK Safety Tech Sector: 2021 Analysis* (Belfast: Perspective Economics, 2021). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/989753/UK_Safety_Tech_Analysis_2021_-_Final_-_190521.pd.

Phippen, A., "Age Verification and Online Pornography – An Effective Safeguarding Approach?", *Entertainment Law Review* 2016 (27(5)), 167–171.

Reed, C., *Making Laws for Cyberspace* (Oxford: Oxford University Press, 2012).

Revealing Reality, *D2.4 Understanding of User Needs and Problems* (London: Revealing Reality, 2021). https://euconsent.eu/project-deliverables/.

Revealing Reality, *Families' Attitudes Towards Age Assurance* (London: Revealing Reality, ICO and Ofcom, 2023). https://revealingreality.co.uk/families-attitudes-towards-age-assurance.

Sas, M., and Mühlberg, J. T., *Trustworthy Age Assurance? A Risk-Based Evaluation of Available and Upcoming Age Assurance Technologies from a Fundamental Rights*

Perspective (Brussels: The Greens/EFA Group at the European parliament, 2024). https://www.greens-efa.eu/files/assets/docs/age_assurance_v2.1.pdf.

Shaffique, M. R., and van der Hof, S., *Research report: Mapping age assurance typologies and requirements, Commissioned by the Directorate-General for Communications Networks, Content and Technology, Better Internet for Kids* (BIK), 2024. https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements.

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S. and Hasebrink, U., *EU Kids Online 2020: Survey Results from 19 Countries* (London: EU Kids Online, London School of Economics and Political Science, 2020). DOI: 10.21953/lse.47fdeqj010fo.

Smirnova, S., Livingstone, S. and Stoilova, M., *Understanding of User Needs and Problems: A Rapid Evidence Review of Age Assurance and Parental Controls* (Athens: euCONSENT, 2021). http://eprints.lse.ac.uk/112559.

Stoilova, M., Livingstone, S. and Nandagiri, R., "Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy", *Media and Communication* 2020 (8(4)), 197–207. DOI: 10.17645/mac.v8i4.3407.

Stoilova, M., Bulger, M. and Livingstone, S., "Do Parental Control Tools Fulfil Family Expectations for Child Protection? A Rapid Evidence Review of the Contexts and Outcomes of Use", *Journal of Children and Media*, 2023. https://www.tandfonline.com/doi/full/10.1080/17482798.2023.2265512.

Third, A., Livingstone, S. and Lansdown, G., "Recognising Children's Rights in Relation to Digital Technologies: Challenges of Voice and Evidence, Principle and Practice", in M. Kettermann, K. Vieth and B. Wagner (eds.), *Research Handbook on Human Rights and Digital Technology* (Cheltenham: Edward Elgar, 2019), 376–410. https://eprints.lse.ac.uk/119869/.

UN (United Nations), *United Nations Convention on the Rights of the Child*, Resolution 44/25 of 20 November (1989). www.unicef.org.uk/what-we-do/un-convention-child-rights.

UN, General Comment No. 25 on *Children's Rights in Relation to the Digital Environment* (Geneva: Committee on the Rights of the Child, 2 March 2021). https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.

UNICEF (United Nations' Children's Fund)/The Danish Institute for Human Rights, *Children's Rights in Impact Assessments: A Guide for Integrating Children's Rights into Impact Assessments and Taking Action for Children* (Copenhagen: UNICEF and The Danish Institute for Human Rights 2013). www.unicef.ca/sites/default/files/2019-01/Childrens-Rights-in-Impact-Assessments.pdf.

van der Hof, S. and Lievens, E., "The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR", *Communications Law* 2018 (23(1)), 33–43.

van der Hof, S. and Ouburg, S., *Methods for Obtaining Parental Consent and Maintaining Children Rights* (Leiden: University of Leiden, 2021).

van der Hof, S. and Ouburg, S., "'We Take Your Word For It' – A Review of Methods of Age Verification and Parental Consent in Digital Services", *European Data Protection Law Review* 2022 (8(1)), 61–7. DOI: 10.21552/edpl/2022/1/10.

van der Hof, S., Lievens, E. and Milkaite, I., "The GDPR and Children's Personal Data", *Oxford Encyclopaedia of EU Law* (*OEEUL*) (Oxford University Press, 2022a).

van der Hof, S., van Hilten, S., Ouburg, S., Birk, M. V. and van Rooij, A. J., "Don't Gamble With Children's Rights – How Behavioral Design Impacts the Right of Children to a Playful and Healthy Game Environment", *Frontiers in Digital Health* 2022b (4). DOI: 10.3389/fdgth.2022.822933.

van Hoof, J., "The Effectiveness of ID Readers and Remote Age Verification in Enhancing Compliance with the Legal Age Limit for Alcohol", *The European Journal of Public Health* 2016 (27(2)), 357–359. DOI: 10.1093/eurpub/ckw183.

van der Maelen, C., "Online Verification Mechanisms in the Personal Data Protection Framework: A Battle for the Ages?" (Amsterdam: Privacy Conference, 2018).

van der Maelen, C., "The Coming-of-Age of Technology: Using Emerging Tech for Online Age Verifications", *Delphi – Interdisciplinary Review of Emerging Technologies* 2019 (2(3)), 115–121. DOI: 10.21552/delphi/2019/3/4.

Williams, R., Derrick, J., Liebman, A., LaFleur, K. and Ribisl, K., "Content Analysis of Age Verification, Purchase and Delivery Methods of Internet e-Cigarette Vendors, 2013 and 2014", *Tobacco Control* 2018 (27(3)), 287–293. DOI: 10.1136/tobaccocontrol-2016-053616.

Yar, M., "Protecting Children from Internet Pornography? A Critical Assessment of Statutory Age Verification and Its Enforcement in the UK", *Policing: An International Journal* 2020 (43(1)), 183–197. DOI: 10.1108/PIJPSM-07-2019-0108.

Zagal, J. P., Bjork, S. and Lewis, C., "Dark Patterns in the Design of Games", *FDG* (*Foundations of Digital Games*) *Conference* (Chania, Greece: FDG, 14–17 May 2013). www.fdg2013.org/program/papers/paper06_zagal_etal.pdf.