GROWING UP IN AN ONLINE WORLD: OPEN RIGHTS GROUP CONSULTATION RESPONSE

Table of Contents

Executive Summary

Age-gating was implemented in 2025 as a limited mechanism aimed primarily at restricting children's access to pornographic content online. Within a short period of time, its scope has rapidly expanded. We have seen age checks introduced across online gaming services, app stores, social media platforms, and other general online services. Proposals within this consultation would extend age-gating requirements across even larger areas of the internet, potentially including social media platforms, VPN services, and even static informational websites.

At the same time, the consultation appears to approach social media harms in relative isolation, without adequately adopting the systems-based approach that Government guidance increasingly recommends for complex societal problems[1]. Children's mental health outcomes are shaped by a broad and interconnected set of factors including family circumstances, educational pressures, economic insecurity, social isolation, sleep disruption, community decline, and wider cultural and technological changes. Social media often reflects, amplifies, or interacts with these underlying real-world conditions rather than operating as a single isolated causal

1 https://www.gov.uk/government/publications/systems-thinking-for-civil-servants

driver. Focusing narrowly on platform access risks oversimplifying a far more complex problem.

The potential consequences of large-scale age-gating and restrictions on children's online participation are also not yet well understood. Online platforms can provide important social connection, educational opportunities, identity exploration, peer support networks, and access to information, particularly for vulnerable or isolated young people. For some people with disabilities online platforms are particularity relied upon. Restricting access without fully understanding these trade-offs may create unintended harms while failing to address the deeper structural causes of poor mental health outcomes.

The risks of expanding age-gating are also very real. Emerging evidence further demonstrates that age-gating systems are frequently far less privacy-preserving than presented to the public, remain ineffective at preventing determined young people from accessing online services. The growing reliance on age assurance mechanisms also risks normalising identity verification across the open internet, with significant implications for privacy, anonymity, freedom of expression, and access to lawful information.

While "safety-by-design" measures may mitigate certain categories of harm, they are not sufficient on their own because they do not adequately address the wider structural and market incentives that shape online environments. Rather than treating social media and youth mental health as isolated policy problems, the Government should adopt a broader systems-based approach that recognises the wider social, economic, technological, and market forces contributing to online harms and poor mental health outcomes. This should include greater scrutiny of the attention economy business model, engagement-driven recommender systems, platform lock-in that restricts meaningful user choice, and the lack of investment in interoperable, community-driven, and public interest alternatives to dominant technology platforms.

Most proposals involve privacy harming digital ID checks.

Most of the proposals would require platforms to introduce what is refereed to by Government as 'age-verification', but what we call digital ID checks. There is an assertion that this technology is privacy preserving. Yet the academic consensus among security experts says otherwise. In an open letter, 371 security and privacy

academics across 29 countries stated the technologies being rolled out are not effective and carry significant risks[2].

Security researchers have demonstrated that services one by Yoti are extensively tracking users without consent, likely in violation of the EU General Data Protection Regulation (GDPR)[3]. The Spanish Data Protection Authority fined Yoti 950,000 euros.[4]Real-world deployments of this technology can't keep people's data safe, as evidenced by Discord's data-leak.[5] This technology is contributing to increased cybercrime costs to the economy, and tangible privacy and psychological harms to individuals. Because this technology is in practice linking people's identities to online accounts it is more accurate to call it a digital ID check.

The problems with privacy harming online Digital ID checks are exasperated by the Government's refusal to come up with a regulatory scheme to ensure high standards within the Industry, and the ACCS' claim that metadata should be collected alongside age proofs[6] ORG has previously made the case for a regulatory scheme to cover these age-checks[7]. This was a proposals that was supported by the Age Verification Providers Association, but correspondence about the proposal did not receive a reply from the Department.

Freedom of expression, and psychological harms arising from restrictions

Placing content that is lawful to access offline, behind an online age-gate is a restriction on people's freedom of expression rights. Access to information is dependent on the 'approval' of a third-party. Restricting people's freedom in this manner cause psychological harms to some individuals. This harm takes the form of anxiety, hyper-vigilance, self-censorship, fear, identity suppression, and social

2 https://csa-scientist-open-letter.org/ageverif-Feb2026 Joint statement of security and privacy scientists and researchers on Age Assurance

3 https://mint-secure.de/dataprotection-it-security-risks-with-ageverificationapp-yoti/ Data protection and IT security issues with age verification app „Yoti"

4 https://www.biometricupdate.com/202603/spains-aepd-fines-yoti-1-1m-for-biometric-data-handling-violations Spain's AEPD fines Yoti $1.1M for biometric data handling violations

5 https://www.bbc.co.uk/news/articles/c8jmzd972leo ID photos of 70,000 users may have been leaked, Discord says

6 https://www.biometricupdate.com/202605/accs-says-reusable-age-check-systems-must-establish-provenance ACCS says reusable age check systems must establish provenance

7 https://www.openrightsgroup.org/publications/regulating-age-verification/ Regulating age-verification

withdrawal[8]. Neurodiverse children, most notably those with autism and ADHD are more likely to spend time online compared to their neurotypical peers, habits which can persist into adulthood.[9] The International Association of Privacy Professionals (IAPP) notes that digital communities offer particular attractions for neurodivergent people: more structure and control over interactions, reduced emphasis on non-verbal communication, and greater ease in finding communities of shared interest[10]. Excluding these people from these online spaces will harm them more than neurotypical indivduals.

Open Rights Groups has received correspondence from supporters and members explaining how age-gates and restrictions online are harming their mental health. For us these harms are not abstract but a tangible result of the policies implemented and being proposed. The Government should conduct an equalites impact assesment that considers the specific harms to people with certain disabilities platform bans would cause.

Privacy is not only a fundamental human right in a legal sense, but a personal psychological need. There is extensive academic literature on the psychological harms of freedom of expression restrictions and surveillance can cause[11]. These harms are particular felt by marginalised groups such as neurodiverse individuals, people with disabilities[12], refugees fleeing oppressive regimes, or victims of stalking and harassment.

We think it's also important to highlight that Children are holders of freedom of expression rights under international human rights law, including Article 13 of the United Nations Convention on the Rights of the Child[13]. This article protects

---

8 https://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling-effects-online-comparative-case Jonathon W. Penney, (2017) Internet surveillance, regulation, and chilling effects online: a comparative case study

9 Ra, C.K., Cho, J. & Stone, M.D. (2018). "Association of Digital Media Use With Subsequent Symptoms of Attention-Deficit/Hyperactivity Disorder Among Adolescents." JAMA, 320(3), 255–263. https://doi.org/10.1001/jama.2018.8931

10 Wallace, P., Boers, E., Ouellet, J., Afzali, M.H. & Conrod, P. (2023). "Social media use and ADHD-related behaviours in adolescents." *Scientific Reports*, 13, 18108. https://doi.org/10.1038/s41598-023-44105-7

11 https://link.springer.com/article/10.1007/s12142-024-00727-6 Niclas Rautenberg (2024) Making Tangible the Long-Term Harm Linked to the Chilling Effects of AI-enabled Surveillance: Can Human Flourishing Inform Human Rights?

12 Malik, A. S., Acharya, S., & Humane, S. (2024). Exploring the Impact of Security Technologies on Mental Health: A Comprehensive Review. *Cureus*, 16(2), e53664. https://doi.org/10.7759/cureus.53664

13 https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child UN Convention on the Rights of a Child

children's rights to seek, receive, and impart information and ideas through any media of their choice. Restricting freedom of expression rights can cause direct harms to the children the policies are designed to help.

The UK is a signatory to the UNCRC, and the UN Committee on the Rights of the Child. The committee has repeatedly stated that children's digital access and online participation are integral to the exercise of these rights, including access to education, community, identity formation, and social participation.

Broad restrictions on access to social media or online communication platforms are likely to disproportionately harm LGTBT, disabled children and young people, including those with conditions such as Cystic Fibrosis, who are often medically advised not to meet others with the same condition in person because of cross-infection risks[14]. For many disabled or chronically ill young people, online spaces are not simply recreational platforms but essential environments for friendship, peer support, self-expression, and participation in public and social life.

Age-gates don't work and have a circumvention problem

Emerging evidence from Australia is that social media bans have not been effective[15]. Young people are simply finding ways to circumvent the ban. It's clear if parents want to keep children off social media they will not be able to rely on a ban to achieve this.

The measures young people are using include tricking biometric age estimation with disguises, logging on with a parents or older siblings account, migrating to less regulated spaces or more obscure platforms or protocols not following regulations or using alternative technologies such as ToR browser or VPNs to try and evade bans.

This suggests that age-gating likely only has a limited use in preventing unintentional access, for example of a child stumbling across pornography, rather than preventing determine teenagers who want to access a service. A similar result can be achieved by basic parental control software, or ISP level content filters. It should also be noted that a survey by Internet Matters survey found that 32% of

14 https://www.cysticfibrosis.org.uk/news/not-being-able-to-meet-each-other-is-one-of-the-hardest-parts-of-living-with-cf-phoebes-story "Not being able to meet each other is one of the hardest parts of living with CF" : Phoebe's story

15 https://fortune.com/2026/04/25/australia-social-media-ban-isnt-working-teens-sidestepping-restrictions/ Most Australian teens admit the social media ban isn't working as they try to sidestep age verification blocks with face masks and their parents' IDs

children had bypassed age checks, while concern about circumvention rose to 73% among parents of "vulnerable children.[16]" This suggest age checks are particular ineffective as in intervention for the most vulnerable children the intervention is meant to support.

When young people circumvent age-gates, they are more likely to find themselves in online spaces that are not designed with children in mind. There is a risk that a platform that relies heavily on age-gating may assume that no children are present on the service, and parents might wrongly belie age-gates precent children accessing content.

If those that provide internet services, and parents harbour a false believe that children are not on the service then this increases the risk that other harm mitigation measures will not be put in place. Why would a parent talk to their child about social media if they believe they can't access it? Why would a platform design a safe space for young people when they can claim only adults are on it?

Harms that arise from restricting VPNs

The debate around whether to restrict young people's access to VPNs focuses on the technologies ability to avoid geo-blocks on content. Unlike the fake moustaches or masks young people are using to trick facial estimation technologies VPNs might appear an easier target to clamp down on.

However as ORG sets out in our briefing on VPNs, [17] they have an important role as a cybersecurity tool for both adults and young people. In this sense restricting young people's access to their ability to use a VPN to circumvent an age-gate would also restrict their access to the cybersecurity benefits of a VPN. Preventing young people's access to VPNs would increase their risk of experiencing other online harms such as online stalking, sexploitation or grooming.

As with other circumvention methods a better approach would likely be to educate young people as to why certain types of content are not appropriate for their age-group, also to improve support for young people when they do experience harms online.

It is worth noting that many of the most oppressive regimes around the world have for years tried to wage a war on VPN use in their countries, as they do not want their

16 https://www.internetmatters.org/wp-content/uploads/2026/04/Internet-Matters-Online-Safety-Act-Report-May-2026.pdf

17 https://www.openrightsgroup.org/publications/briefing-vpns-and-the-online-safety-act/ Briefing VPNs and the Online Safety Act

citizens to have free access to information. These efforts have had mixed results with many citizens in Iran, China and Russia still being able to access VPNs.

If the Government did pursue a policy of trying to restrict VPN access then the likely impact is further more extreme circumvention methods. This could include use of protocols such as ,Tor, Obfs4, Snowflake, Shadowsocks, V2Ray, Trojan, HTTPS/WebSocket tunnelling, SSH tunnelling, Matrix, XMPP, I2P. It's probably more sensible to keep young people on TCP/IP protocols where Government and Ofcom can at least talk to the main platforms and providers.

Don't harm the small services trying to build better

Many Neitzens have been concerned about the state of large big tech platforms before the Online Safety Act was a twinkle in any politicians eye. For years technologists, community leaders, geeks, and visionaries have been trying to build a better internet.

These alternative online spaces are normally motivated by a desire to create community around common interest or shared community spaces. One example might be small community forums based around football clubs such as the Sunderland FC forum. Within the gaming community many of these services are run by preservationists who are keeping old video games running and preventing the loss or destruction of cultural works.

Scotland is an example of a nation with a high number of small community run spaces ,built around different rural or island communities. In addition to the examples already given there exists both a Welsh and Scottish Mastodon servers. Mastodon is a decentralised social media network that operates on the Fediverse using the ActivityPub protocol. Although it can't be said that such networks are harm free, their community-led approach, and community moderation does result in fewer harms than larger platforms dominated by capturing user attention to sell advertising.

It is therefore unfortunate that attempts to regulate online spaces for the purposes of safety are having the most determiner impacts on the very small communities that are trying to build better alternatives.

Proposals in this consultation, such as restricting young people's access to social media, is not something that these small community spaces will be able to comply with. There are a variety of reasons for that. A primary one being the cost of operating and installing digital ID checks on all users. Another being the increased

privacy, technical and administrative responsibilities and liabilities that arise from these measures.

Open Rights Group tries to document the small sites and and services that have been forced to close already due to the Online Safety Act with our 'Blocked' project[18]. It seems as if policy is being written with large platforms in mind and is catching small communities in the regulatory drag net. It's perhaps not so much that policy makers don't regret that this is happening, but they have not cared enough to put I place measures that would prevent it happening. The issue with small sites and services closing was picked up by some MPs when a petition to repeal the Online Safety Act was debated last December 2025 in parliament[19].

One solution to this problem would be to have a small and community services exemption from some of the restrictions and requirements being imposed on the large big tech platforms. ORG has drafted an amendment to existing laws that could facilitate this change. When considering how to use the new powers to restrict services granted by the Children and School's Wellbeing Act we urge civil servants and the Minster to please consider these small community services.

If Government were to recognise the benefit of small community websites and servers then it could adopt a policy of even nurturing such civically minded efforts. For example just as there is already a Welsh and Scottish Mastodon server. There is nothing to stop educational establishments, local authorities, or Government Departments also playing an active role in building positive and constructive online spaces. We encourage the Government not just to ban children and restrict, but instead build better online spaces for young people.

GDPR Article 8 is doesn't work as a regulatory mechanism for broad online age-gating

The consultation raises important questions about age assurance and children's experiences online. However, Open Rights Group does not believe that Article 8 of the UK GDPR provides an appropriate framework for creating broad online age-gating requirements.

Article 8 was designed specifically to address situations where consent is relied upon as the lawful basis for processing a child's personal data in relation to information society services. However, consent is only one of several lawful bases for processing personal data under UK GDPR. Many online services instead rely on

18 https://www.blocked.org.uk/osa-blocks Blocked website

19 https://hansard.parliament.uk/commons/2025-12-15/debates/DA0F7CFE-CCED-4864-BCCF-160E0AF56F92/OnlineSafetyAct2023Repeal Online Safety Act 2023: Repeal debate

other legal bases such as legitimate interests, contractual necessity, or legal obligations.

As a result, attempting to use Article 8 as a general-purpose online age-gating mechanism risks creating an incoherent regulatory framework where age assurance obligations depend not on the nature of the service or the risks presented to children, but on which lawful basis a platform chooses to rely upon for data processing.

There is also a risk that expanding the use of Article 8 in this way would increase pressure for widespread deployment of intrusive age assurance technologies across the internet.

In practice, implementation of the ICO Children's Code has already contributed to increased use of facial age estimation and other biometric age assurance systems by online platforms[20]. This has resulted in growing numbers of children being required to provide biometric data to third-party age assurance providers, many of which are overseas companies processing highly sensitive personal data which creates significant cybersecurity risks to British citizens.

This approach creates a concerning dynamic where measures intended to protect children's privacy and wellbeing may instead normalise routine biometric checks and identity verification as a condition of accessing lawful online services. The result is more personal data entering the advertising and recommender systems that are exasperating online harms, and feeding AI training models.

DSIT should therefore avoid treating GDPR consent mechanisms as a substitute for a coherent online safety framework. Questions around harmful design, recommender systems, behavioural profiling, and platform incentives should be addressed directly, rather than indirectly through data protection consent provisions that were not designed to function as universal online age gates.

Addressing the commercial incentives behind harmful design

The consultation rightly raises questions about the role that platform design features play in shaping children's online experiences. However, it is important to recognise that many harmful online experiences do not arise from isolated design choices alone, but from the interaction between platform design, user-generated content, and the commercial incentives that shape platform behaviour.

20 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/03/joint-statement-from-ico-and-ofcom-on-age-assurance/ Joint statement from ICO and Ofcom on age assurance

Mike Masnick illustrated this dynamic in a thought experiment published by TechDirt[21]:

> "Here's a thought experiment: imagine Instagram, but every single post is a video of paint drying. Same infinite scroll. Same autoplay. Same algorithmic recommendations. Same notification systems. Is anyone addicted? Is anyone harmed? Is anyone suing?"

This example highlights an important limitation of approaches focused solely on regulating individual design features. Features such as autoplay, infinite scroll, recommendation systems, and notifications become harmful primarily when combined with content and an economic incentive to maximise user attention and engagement.

The consultation asks what interventions could create safer and more positive online experiences for children, it's therefore important to consider the commercial incentives driving platform behaviour. Many large platforms operate on surveillance advertising business models that depend on maximising engagement, data collection, and time spent on-platform. This creates structural incentives to promote emotionally stimulating, compulsive, or highly attention-retentive content. This incentive simply does not exist in the same way on sites created with educational, values or community driven goals.

We are concerned attempts to regulate harmful design through restrictions on individual features alone risk creating a continual cycle of regulatory "whack-a-mole", where platforms adapt by introducing new engagement-maximising features that fall outside existing rules. This could occur while at the same time making it difficult for community driven small projects to comply with rules as to what features are or are not allowed.

Policy interventions should therefore focus not only on individual design choices, but on the underlying business models and incentive structures that drive harmful platform behaviour.

One important intervention would be restricting or phasing out surveillance advertising models based on extensive behavioural profiling. Platforms such as Meta, TikTok, and Google derive significant revenue from targeted advertising systems that reward prolonged engagement and large-scale personal data collection. Limiting the collection and use of personal data for advertising purposes

---

21 https://www.techdirt.com/2026/03/26/everyone-cheering-the-social-media-addiction-verdicts-against-meta-should-understand-what-theyre-actually-cheering-for/ Everyone Cheering The Social Media Addiction Verdicts Against Meta Should Understand What They're Actually Cheering For

would reduce the commercial incentive to develop recommendation systems and platform features optimised primarily for engagement rather than user wellbeing. It would also create a more even playing field with other forms of advertising that exist within the media landscape.

ORG explores alternative approaches in our report *Consent Without Paying: Alternatives to Meta's Surveillance Advertising Models*[22]. These alternatives demonstrate that digital services can operate successfully without relying on business models that incentivise harmful engagement-driven design.

Interoperability and user control as systemic safety interventions

Adopting a systems-based approach to online harms would also require greater consideration of structural market interventions, including interoperability obligations, open standards, portability, and measures to reduce platform lock-in. Many harms associated with large online platforms are not simply the result of individual pieces of content, but of market structures and business incentives that reward surveillance, engagement maximisation, and dependency.

DSIT and its Ministers should consider the role that platform concentration and user lock-in play in exacerbating online harms. A small number of dominant platforms benefit from powerful network effects that make it difficult for children, families, and communities to move to safer or more privacy-friendly alternatives without losing access to their social networks and online communities. We could even go so far as to say the failure to regulate the internet as a market, and to allow the dominance of a few big tech mega-corporations has been a suboptimal outcome.

Interoperability measures could help address these structural problems by increasing user choice and reducing dependence on engagement-driven platforms. Our report *'Making platforms accountable – empowering users and creating safety'* [23] goes into greater details on how this could be done.

Interoperability is a term that seems entirely lacking from British discourse on internet regulation despite our best efforts to talk about it. Perhaps a more simple way of explaining the concept would be to talk about 'social media account switching'. This could take the form of horizontal interoperability, as the EU is

22 https://www.openrightsgroup.org/publications/consent-without-paying-alternatives-to-metas-surveillance-advertising-models/ 2025 Consent without paying alternatives to Metas surveillance advertising models

23 https://www.openrightsgroup.org/publications/making-platforms-accountable-empowering-users-and-creating-safety/ (2025) Making platforms accountable – empowering users and creating safety.

undertaking with messaging services via the Digital Services [24]. The purpose of horizontality interoperability is to lower barriers to switching between services. Interoperability has two axis so we can also talk about vertical interoperability. Campaigns slogans for this include 'taking back control of our feeds'.

Taking back control of feeds means allowing third-party clients, user-controlled recommendation systems, and interoperable moderation tools. All of which would give users and families greater control over how online content is ranked, filtered, and recommended. These approaches would support safer online experiences both by increasing user agency, but more importantly creating competitive pressure for platforms to improve safety, privacy, and wellbeing to retain users.

We would also welcome the opportunity to sit down with officials to discuss interoperability in more detail, including how it could support a healthier and safer online environment without resorting to blunt restrictions on access and participation.

At present, there appears to be growing momentum behind social media bans and age-gating measures as the primary policy response to online safety concerns. However we predict that these measures will ultimately prove ineffective. Because they are easily circumvented, undermine privacy, or fail to address underlying platform incentives. As such policymakers will inevitably need to consider alternative structural solutions.

Interoperability deserves serious consideration as part of that future conversation. Rather than concentrating power further in a small number of dominant platforms, it offers the possibility of greater user choice, stronger competition, and safer, more accountable online spaces by design.

We would be very happy to engage further with officials on how such approaches could work in practice.

24 https://www.europarl.europa.eu/topics/en/article/20211209STO19124/eu-digital-markets-act-and-digital-services-act-explained EU Digital Markets Act and Digital Services Act explained