SLAUGHTER AND MAY

19 May 2026

Protecting children online: how is the law changing, and where will it go?

The law tends to move slowly – except when it doesn't. There are times when legislators snap into action and laws are made quickly – usually in times of political ferment, when issues grip policymakers and events assume their own momentum. For child safety online, we are living in that moment. After years of relative stability in the regulation of online safety, there is a sudden intensity of action.

Proponents will say this is a snap of consciousness, a long-delayed drive towards definitive action. Critics will say it is collective political inflation, with governments suddenly afraid of looking careless by comparison – and racing towards interventions without proper thought.

What is happening, and where will it end up? And will it get the right results?

Why now?

The first question is why now. This is a fair question, because whilst there have been a handful of distinct issues, there has been no sudden, widespread increase in the risk that would explain the current level of policy activity. Indeed, the key online regulations in the EU and the UK have essentially been in force since 2024.[1]

The clearest recent policy trigger is Australia's prohibition on social media use for under-16s. In December 2025, Australia became the first country in the world to ban under-16s from using ten major platforms, including Facebook, Instagram, TikTok, Snapchat, X, and YouTube. Those platforms are required to take "reasonable steps" to prevent users under 16 from creating or maintaining accounts, with potential penalties of up to AUD $49.5 million for serious or repeated breaches.

This was closely watched across Europe, and Australian delegates have since been travelling to meet with EU and UK policymakers to discuss their experiences. The impact of that ban in Australia is mixed (as we discuss below) – but it has triggered a domino effect in the EU, with most Member States now seriously exploring outright prohibitions for minors,[2] and France and Greece leading calls for EU-wide action. It has also intensified the enforcement of age assurance rules from multiple angles, as regulators have looked to existing rules to harden positions on age-gating (as we outline below).

The political context is clear – and difficult. Few issues command such broad public agreement as the safety of children, so how can individual governments (and regulators) "go softer" than others on such sensitive issues?

What are the issues – and which regulators are pursuing them?

The policy debates are now coalescing around three areas:

1. Outright prohibitions for minors;
2. Stronger age assurance for accessing certain services; and
3. Broader issues of platform design and experiences (including so-called "addictive" design).

These issues are spread across multiple regulators, in some cases with overlapping jurisdiction:

- Age assurance is a feature of online safety rules and of privacy rules. In the EU, the European Commission (the "**Commission**") enforces the

[1] The Digital Services Act in the EU came fully into force in February 2025, and the child safety duties under the UK's Online Safety Act came into force in July 2025.

[2] The exact age threshold for the application of the social media bans under consideration varies across Member States (15 in Greece and Poland, for example, versus 16 in Spain and France).

Digital Services Act ("**DSA**") (the main EU-level online safety regulation, which includes rules on age verification) against so-called "very large online platforms" (the targets for most of this enforcement).[3] In the UK, Ofcom enforces the Online Safety Act ("**OSA**"), which has similarities with the DSA, and is actively enforcing age assurance as part of a drive to increase child safety online. At the same time, in both the EU and UK, some privacy regulators (including the UK Information Commissioner's Office ("**ICO**")) have taken enforcement action against platforms for failure to adequately check the age of users (see our blog). Their jurisdiction naturally includes platforms processing personal data (where they meet the relevant territorial requirements), and so there is regulatory overlap with the online safety regulators where the DSA / OSA apply.

- Issues of platform design are addressed in the online safety rules, with the Commission already reaching a preliminary decision around the so-called "addictive" design of TikTok under the DSA (see our briefing). As we have outlined, this was supposed to be a key focus of the Digital Fairness Act ("**DFA**"), but the Commission is already prosecuting these issues within the framework of the DSA. In addition, some aspects of online architecture are also caught by privacy laws, with several privacy regulators having published guidance on so called "dark patterns".

- Any outright bans need to be introduced with new legislation, as online safety rules in the EU and the UK have not, to date, provided for that intervention.[4]

For platforms, this requires a multi-regulator strategy which is intrinsically challenging. Online safety and privacy regulators are investigating the same platforms, sometimes for the same or adjacent issues. Meanwhile, broader policy debates are unfolding at the political level that could rip up the existing rulebook. And all of this is happening in areas where the evidence on relative benefits and harms, and the nature of platform design, is intensely unresolved.

Outright bans – will they happen, and would they work?

In the EU, most Member States are now pursuing plans to restrict children's access to social media. The Commission is also exploring an EU-wide harmonised approach[5]. In a November 2025 report, the European Parliament called for a harmonised EU digital age limit for social media of 16 as the general rule unless parents or guardians give permission, and 13 as an absolute minimum (aligning with the current minimum age for children to consent to their personal data being processed under the EU GDPR).

The UK is also actively considering whether to follow Australia's lead. The Government launched a three-month consultation on 2 March 2026 (closing on 26 May), seeking views on minimum age requirements for platforms, restrictions on potentially addictive features, mandatory overnight curfews, and the role of age assurance technologies in effective implementation.[6] Despite this ongoing work, and under pressure from the House of Lords, in late April the Government agreed to introduce either age or functionality restrictions on social media for under 16s in the next 15 months,[7] with the detail of those measures to be informed by the current consultation. The mechanism for the Government to introduce such measures has been added to the OSA by way of the Children's Wellbeing and Schools Act, which received Royal Assent on 29 April 2026. More specifically, the amendment added a provision to the OSA that provides that the Secretary of State may introduce regulations requiring providers of "*specified internet services*" to prevent or restrict access to their services by "*relevant children*".[8]

The striking thing about the debate is how quickly policymakers have travelled to the most extreme type of intervention – and one that governments across Europe

3 VLOPs include, for example, TikTok, Facebook, Instagram, Snap and YouTube.

4 Although, as detailed further below, the OSA has recently been amended to include a new provision that enables the Secretary of State to introduce regulations requiring providers of "specified internet services" to prevent or restrict access by "relevant children".

5 See the speech delivered on 12 May 2026 by the President of the European Commission, Ursula von der Leyen, to the European Summit on Artificial Intelligence and Children, as discussed further below.

6 In parallel, trials of social media bans, digital curfews and app time limits are being piloted in the homes of 300 UK teenagers.

7 The UK Government has committed to produce a progress report on the topic within three months of the Children's Wellbeing and Schools Act receiving Royal Assent on 29 April 2026, with regulations to be made within 12 months of the report, subject to a six-month extension to be used only in exceptional circumstances.

8 The amendment also requires the Secretary of State to exercise this new power to make such provision as the Secretary of State considers appropriate following the conclusion of the consultation, and, in doing so, to have regard to the consultation responses.

have been resisting until quite recently. In this environment, there is rarely space for dissenting views, or even sensible questions – but three points are important as the law takes shape:

1. First, there is significant disagreement on whether banning children completely from social media is the right thing to do. Several prominent child safety organisations and experts have warned that a blanket ban is not the solution,[9] and there is a serious debate about whether the right approach is prohibition or education. For example, concerns have been raised about a digital "cliff edge",[10] where age restrictions result in children who have had no engagement with social media suddenly using platforms when they turn 16, without having developed any digital literacy. Surely, this argument would say, a managed diet is better than a sudden binge. There is also a significant body of evidence on the benefits of social media (especially for more vulnerable or marginalised children) that is at real risk of being ignored completely, even where it could help in designing new rules effectively.[11]

2. Second, and in this context, prohibition risks undermining the broader policy objective of encouraging safety by design. A key goal of online safety rules is to develop a system of rules and deterrence that encourages platforms to be "better" by design – and to invest in that objective, for the benefit of minors and adults alike. If platforms are banned completely for minors, that could significantly diminish platform incentives to increase overall safety (because minors – as the most direct beneficiaries – would be blocked anyway). This, combined with the risk of circumvention (see below), could mean that bans represent only a single, thin line of defence, while the fundamental issue of platform design goes unresolved.

3. Third, if the bans do happen, they will only be as good as their results. In Australia's case, the bans provoked instant, widespread circumvention, with Australia's eSafety Commissioner finding that around 70% of under-16s who were blocked from the major platforms found ways to maintain access (including by using VPNs).[12] The related risk is that minors disperse to platforms that are either not captured by the prohibitions or do not observe them (there will be a market opportunity here for less scrupulous actors). This is a point made by the major platforms (and therefore liable to be ignored) – but is a legitimate one and has received no coherent response from regulators.[13] All of this will come down to design and implementation. For example, defining a fixed group of banned platforms risks creating a new category of permitted platforms with weaker safety standards (a form of legislative "whack-a-mole"). Better to make the definition "breathe" so that it can respond to emerging risks. And the law would need to confront circumvention directly – setting clear rules around user identification, VPN use and other circumvention issues (see further below).[14]

How will this play out? The EU picture is more complicated than the UK's, because of the presence of the DSA. As a "full harmonisation" measure, the DSA sets the highest threshold for platform rules in the EU. Member State authorities cannot pass different or additional rules (to avoid fragmenting the internal market). This is problematic for policy makers considering a ban, as the DSA does not prohibit the use of platforms by minors (although the Commission is pursuing individual cases on age assurance (see below)).

---

9 A joint statement to this effect was signed by 42 child safety organisation, experts and bereaved families including the NSPCC, the Molly Rose Foundation and the Institute for Strategic Dialogue. The Electronic Frontier Foundation has also criticised bans on minors using social media, as has Michael O'Flaherty, the Council of Europe's Commissioner for Human Rights.

10 See: Children's and online safety campaigners issue joint statement on social media ban for under-16s, 18 January 2026

11 See for example: Nagata JM, Huang O, Hur JO, Li EJ, Helmer CK, Weinstein E, Moreno MA. Health Benefits of Social Media Use in Adolescents and Young Adults, 15 August 2025; and Miller J, Mills K.L, Vuorre M, Orben A, Przybylski A.K, Impact of digital screen media activity on functional brain organization in late childhood: Evidence from the ABCD study, Cortex, 15 November 2023

12 eSafety Commissioner, Social Media Minimum Age: Compliance Update March 2026

13 Although this risk – and the challenges it poses to the effectiveness of any ban – have been recognised. For example, the UK's consultation recognises that "*if minimum age restrictions only apply to a small number of the most popular user-to-user services, this could risk displacing children into other online spaces, including less regulated ones*".

14 Notably, the UK Government's consultation specifically includes questions about VPNs, including whether access to VPNs should itself be age-restricted for children and what the potential impacts of such measures might be on users who rely on VPNs for privacy and security.

The state of the national debate makes this unsustainable, and we think there will be – this summer – a legislative proposal at EU level that accommodates prohibitions at national level (notwithstanding the harmonisation principle).[15] And because it deals in such sensitive terrain, this will only be the first crack in the harmonisation principle under the DSA.

Age assurance – hard lines, soft rules

Alongside the debate on outright bans, we have seen hardening positions on the enforcement of age assurance for online services that are (in theory) age-gated – even if the underlying rules haven't changed:

- Under the DSA, there has been a hardening position against "self-declaration" for age assurance (i.e. where users indicate their age without this being further verified). The Commission, for example, has provisionally found Meta to have breached the DSA for relying on self-declaration (and ineffective reporting tools) to enforce its under-13 restriction. The Commission is investigating Snap for similar issues, including Snapchat's reliance on self-declaration as an age assurance measure, with the Commission suggesting that this "*neither prevents children under the age of 13 from accessing the service, nor adequately assesses whether users are younger than 17 years old, which is necessary to ensure an age-appropriate experience*."

- Under the OSA, Ofcom has also increased its focus on age assurance in alignment with the ICO. The two regulators issued a joint statement in March that explicitly calls on platforms to move away from self-declaration. The ICO has recognised that this will require a change to current practices given that many social media and video sharing platforms have relied on self-declaration to date, as it acknowledged in an open letter to industry in March. This intensifying focus on age assurance has also seen Ofcom expand its OSA enforcement efforts to focus on household name platforms. The regulator called on six platforms most used by children (including YouTube, Instagram and TikTok) to report on their approach to age assurance (and other child protection measures) by the end of April, with Ofcom due to publish a report on their responses this month. The ICO has also expressed an intention to engage with 17 of what it calls high-risk platforms that are primarily relying on self-declaration, as part of its work to drive the adoption of more robust age assurance methods.

- Under privacy rules, there have been several joint statements from data protection authorities ("**DPAs**") calling for the protection of children in an online context, including in the context of AI generated imagery in February (see this blog) and, in late 2024, outlining shared principles on age assurance. The age assurance statement suggests self-declaration will be insufficient other than where there is '*little or no data protection risk to children*'. More recently, in December 2025, the ICO expressly set out that "*self-declaration used in isolation is not appropriate for services likely to pose high risks to children*" in the context of driving compliance with its Children's Code statutory guidance. The ICO went on to fine two companies for failures in this area.[16]

Two aspects of these developments are striking.

First, while "positions" are changing, the hard rules are not. Privacy regulators have now reflected on the latest available age assurance technologies and decided (either by way of statements, or by way of individual enforcement actions) that reliance solely on self-declaration can no longer be justified. In other words, whilst self-declaration was a legitimate approach to age-gating online services, it no longer is. The EU and UK data privacy and online safety regimes require organisations to adjust to evolving risks and technical developments, and so it is not surprising that

[15] The Commission has established a Special Panel on Child Safety Online to advise on protecting minors online and the potential introduction of EU-wide age limits for social media. The panel will deliver recommendations by summer 2026 to guide possible further EU level action. In her keynote speech at the European Summit on Artificial Intelligence and Children on 12 May 2026, President von der Leyen indicated that legislation providing for an EU-wide 'social media delay' for children could be announced this summer, depending on the panel's finding. An alternative (or, more accurately, workaround) could be for Member States to frame their bans as restrictions applying to minors themselves (not to the platforms). Enforcement on platforms can then be managed under the DSA, given that to comply with their existing obligations under the DSA with respect to protection of minors, platforms will need to factor in any age limits for use set by Member States, and, based on Article 28 guidelines published by the Commission, will be expected to use age verification technology to prevent minors below the legal age limit from accessing the service.

[16] Specifically Imgur (£247,590) and Reddit (£14.47 million) in connection with their reliance on prohibitions on under 13s in their terms and conditions and reliance on self-declaration (discussed further in this blog).

the regulators update their advice in this way, as things change. On the one hand this helps the regimes stay relevant, without requiring constant legislative amendments, but on the other hand organisations can be left without real clarity about what is expected of them at any one time.

Second, alignment between data privacy and online safety rules is increasingly important to ensure consistency across these overlapping rulesets. For proper age restriction to be workable in practice, platforms need to be able to effectively establish users' age and be confident that using mechanisms to do so will be viewed as a legitimate and proportionate use of personal data. Recent cross-regulatory statements on age assurance from the ICO and Ofcom in the UK[17], and from Spain's DPA and Digital Services Coordinator, show that some regulators are collaborating in efforts to provide organisations with the certainty they need, but this is not universal. It is therefore clear that data privacy is a key factor in any age assurance solutions that market participants look to use.[18]

Age assurance technologies are increasingly employing cryptographic and other anonymisation techniques to address privacy concerns, with several types of technology seeing adoption (and support from DPAs)[19] and the Commission announcing that its own age verification app is near-ready. But for these technologies to be the solution to age assurance, two things will need to happen: first, there will need to be widespread agreement among privacy and online safety regulators on which technologies satisfy the requirements whilst leaving flexibility for platforms to innovate their own solutions. Second, those technologies will need to be technically fit for purpose (as judged by individual market participants) and not introduce their own risks. Today, neither is the case.

Platform design – narrow findings, wide remedies

On platform design, both online safety and data privacy regulators are increasingly focused on safety by design – and on using the rules to actively shape the ways that platforms operate. Features considered to be "addictive" (e.g., infinite scroll, autoplay, push notifications) and those which are seen to create "rabbit hole" effects, such as highly personalised recommender systems, have come under particular scrutiny for their potential impact on minors (as well as adults).

For example, in February, the Commission provisionally found that TikTok is in breach of the DSA for its "*addictive design*" (see our recent briefing). The Commission is also planning to lay down rules on addictive design in the DFA (discussed in this briefing), with concrete proposals expected in the last quarter of 2026[20]. In the US, addictive features have been the subject of headline-grabbing legal actions against major platforms including Meta, TikTok and YouTube. In the UK, both the ICO and Ofcom are actively scrutinising major social media platforms' recommender systems, with further intervention expected in this area.

It is not surprising to see enforcement cases brought against TikTok, Meta and others under the DSA. Those platforms were always priorities for enforcement, and the DSA was always going to be used for targeting individual organisations. What is surprising is how the current enforcement cases seek to take narrow findings as a pretext for wide remedies – and what this means (and doesn't). Specifically:

- In the provisional TikTok decision (which we explored in depth in our previous briefing), the Commission finds that TikTok's mitigations, "*particularly the screentime management tools and parental control tools, do not seem to effectively reduce the risks stemming from TikTok's*

[17] Developed and issued as part of their participation in the UK's Digital Regulation Cooperation Forum.

[18] Last year, for example, the umbrella body of EU DPAs (the European Data Protection Board) published new guidance reemphasising the importance of data privacy compliance in age assurance, and in March, the Spanish DPA issued a €950,000 fine to leading age assurance tool provider, Yoti, for privacy failings (although this is being appealed).

[19] While the ICO has said its approach is 'tech neutral' - it does not mandate the use of any specific technologies - it has referred to "facial age estimation, digital ID, or one-time photo matching" as examples of current viable technologies for enforcing a minimum age of 13. See also this recent joint statement from the Spanish DPA and Spanish National Markets and Competition Commission, as Digital Services Coordinator, which endorses "non-linkable, privacy-preserving solutions, such as anonymous tokens and the EU Digital Identity Wallet, to ensure the best interests of the child are secured without compromising all users".

[20] According to timings indicated by EU Commissioner Michael McGrath in a session delivered to a Privacy Laws & Business event, Ireland and EU privacy/digital laws: New horizons, on 14 May 2026. It was indicated in that session that the DFA will look to address addictive design practices, including 'dark patterns', unfair personalisation and a restriction on advertising to minors.

addictive design". The logical remedy in those circumstances would be to improve those mitigations (e.g. by implementing stronger tools within the app to reduce usage or strengthen parental controls). But the Commission's remedy is nothing less than to "*change the basic design of [TikTok's] service*", including by "*disabling key addictive features such as 'infinite scroll'*" and reducing personalisation.

- Similarly, in the provisional Meta decision, the Commission finds that Meta's age assurance measures "*do not adequately prevent minors under the age of 13 from accessing their services nor promptly identify and remove them, if they already gained access*." Again, the logical remedy would be to strengthen the age assurance measures to reinforce the policy restriction on under-13 use. But the remedy is much wider: "*the Commission considers that Instagram and Facebook must change their risk assessment methodology, in order to evaluate which risks arise on Instagram and Facebook in the European Union, and how they manifest. Moreover, Instagram and Facebook need to strengthen their measures to prevent, detect and remove minors under the age of 13 from their service*." In other words, a ground-up reassessment of the methodology for assessing substantive risks across Instagram and Facebook (plus better age assurance).

We will need to see the final findings to understand the Commission's full reasoning (and to get a better sense of the evidence), but a reasonable interpretation of these findings is this: that the Commission is using narrow cases as a vehicle for actively and fundamentally reshaping how these platforms work. This is a problem for reasons we've explored before – it attracts serious questions about proportionality, legal certainty, and the distortive effects of intervention on market competition. But above all, it is unlikely to advance the broader objectives of the DSA. Why?

The Commission hopes (indeed, says) that these individual cases will set a standard – that other platforms will take note and adjust. That is how enforcement creates deterrence. But this reasoning breaks for the simple reason that all platforms are different, and the DSA regulates them differently.

Under the DSA, all platforms represent their own specific risks – and therefore their own compliance profile. The Commission would agree with this – it is central to the DSA's architecture, particularly in the context of Articles 34 and 35 (which require platforms to undertake their own assessments of the specific systemic risks caused by their services). In this context, enforcement is unlikely to create effective deterrence, because platforms will often find ways of differentiating themselves from a given case (and often legitimately). It will generally be possible for platforms to take the view that their services present a different risk to, for example, TikTok's (and they will be commercially incentivised to reach that view). If, for example, the Commission does require TikTok to disable infinite scroll or autoplay in the EU, it is exceptionally unlikely that other platforms would voluntarily do the same. This is different to other areas of EU law, where individual cases can create widely applicable rules (for example, an antitrust case against a particular pricing practice, from which general principles can be derived).

This is legislation by enforcement, or, indeed, worse: mere enforcement, with no consequences for anyone other than the target.[21] If the intention of the DSA was only to target specific platforms, that was the right of the EU legislature. But that is not what the DSA says, and it is not the basis of these enforcement cases – and that not only generates confusion and uncertainty but could prove self-defeating as a means of increasing safety online.

What next?

Given the intensity of political focus, it seems likely that we will see significant legislative interventions in the coming months across the EU and the UK. A broader, deeper debate on these issues, and the development of consistent rules on, for example, platform design features, age assurance solutions, and the types of behavioural indicators and relevant data benchmarks that should inform what is legal and not, would have been the better solution.

The risk is that the first comes at the cost of the second – and that significant, politically-driven interventions take the place of the harder work of developing consistent, workable rules in these markets that have a better chance of achieving the long-term policy aims.

[21] Except the potential for other platforms to benefit from dispersing users, as we have outlined before.

Contact

Laura Houston
Partner
T: 07825006706
E: Laura.Houston@slaughterandmay.com

Rebecca Cousin
Head of Privacy, Senior Consultant
T: 07795613789
E: Rebecca.Cousin@slaughterandmay.com

Will Manley
Head of Digital Regulation
T: 0032493406939
E: Will.Manley@slaughterandmay.com

Bryony Bacon
Senior Knowledge Lawyer
T: 07775411392
E: Bryony.Bacon@slaughterandmay.com

London
T +44 (0)20 7600 1200
F +44 (0)20 7090 5000

Brussels
T +32 (0)2 737 94 00
F +32 (0)2 737 94 01

Hong Kong
T +852 2521 0551
F +852 2845 2125

Beijing
T +86 10 5965 0600
F +86 10 5965 0650