ONLINE SAFETY ACT NETWORK

EVIDENCE TO SIT COMMITTEE INQUIRY INTO SOCIAL MEDIA AGE RESTRICTIONS

Summary

1. This evidence is submitted to the SIT committee ahead of its one-off inquiry session into Social Media Age Restrictions and is provided ahead of the appearance of Prof Lorna Woods OBE, the Network's expert legal adviser, to give oral evidence.

2. This submission provides some analysis on the effectiveness of such an approach and the difficulties from a legal perspective, which Prof Woods would be happy to expand on further in her oral testimony.

3. It is perhaps no surprise that calls for restrictions on children and teenagers' access to social media have reached a crescendo since the start of the year. Since January, we have seen ongoing[1] and pervasive harms online[2] impacting young people. It seems that parents feel that the online world is getting less safe for children, despite the Online Safety Act (OSA), and Parliamentarians have been frustrated at the speed of Ofcom's implementation and the Government's refusal - until recently - to consider where the Act and its enforcement might be strengthened.

4. An absolute ban on social media for under-16s is not a silver bullet, however. Many civil society organisations, including many within the Online Safety Act Network, have warned that such an approach fails to address systemic issues present in the design of platforms. Moreover, solely relying on a ban, however structured, leaves the protection

---

1 https://www.childrenscommissioner.gov.uk/resource/a-healthy-influence-childrens-exposure-to-appearance-changing-products-online/

2 https://mollyrosefoundation.org/wp-content/uploads/2026/01/Resolver-Critical-Harm-Intelligence-Briefing-Weaponised-Loneliness.pdf

of children relying on a single mechanism, and no ban is completely effective.

5. In response to both the parental campaigns and subsequent Parliamentary pressure, the Government announced in January they would launch a consultation and "National Conversation" on children's online safety, the details of which were published on 2 March. This seeks to address ongoing concerns about children's safety in the UK and explores new interventions including those to tackle addictive design and harm from AI chatbots.

6. This is the first major consultation since the Online Safety Act was passed, over two and a half years ago but the terms of it risk making that National Conversation a very narrow one; a binary choice between a handful of, admittedly relevant, considerations the Government has identified which improve children's wellbeing and online lives, or restrictions for children being on those platforms in the first place. This framing overlooks some of the harder questions about the causes of risk and harm online. As currently framed, it fails to address the systemic issues at the heart of online harm.

7. In this evidence, we put forward some different approaches on how we might understand "bans", issues arising from the Australian approach for the Committee's consideration, as well as proposals to strengthen the Online Safety Act with a few technical amendments to the Act but particularly the need for safety by design.

Approaches to Bans and Access Restrictions

8. The term "ban" might be taken to cover a range of restrictions. At the extreme end, it could refer to an absolute prohibition on a product or a service - for example, certain single-use plastic items. More common are access restrictions, which can be seen, for example, in the context of pornography (including as regards primary priority content harmful to children in the Online Safety Act) and alcohol (limited by age), hosepipe bans (time and context restrictions) or prescription medicines (restricted by context of use). Product safety rules can be seen as a form of conditional ban: where the products meet the safety thresholds, they are permitted but the ban does not apply to all products in a category.

9. Bans can be deployed in different ways too. In some contexts the ban is the primary mechanism for achieving the policy aim; more often we see bans operating in conjunction with other (safety) regulations - as in the case of product safety. There the ban might be seen as part of an enforcement mechanism. Finally, perhaps as a sub-set of

enforcement, bans or restrictions on access could be seen as part of the penalty for a non-compliant product or service. Arguably, the business disruption measures in the Online Safety Act could be seen in this way.

10. In the context of social media, messaging apps and online games, bans or restrictions could occur at a range of levels in the distribution chain, with different impacts on access and on users' rights. Restrictions could be imposed at the level of communications infrastructure (e.g. when the Internet is blocked), or through a ban on the interfaces - that is smart phones, tablets, etc. Access could be restricted to services (e.g. the blocking of a particular site) or category of services. Sometimes restrictions distinguish between the commercial distribution of a product or service and private use; we can also see that there are restrictions on advertising, which is another way of controlling commercialisation of a product (see e.g. less healthy foods; tobacco products). Restrictions might be time-based (e.g. the watershed on broadcast television or digital curfew) or quantity based (number of paracetamol sold without a pharmacist; screen time limits).

11. There is a difference between the blocking of a site as a result of state action and a service provider choosing to geoblock itself to avoid a regulatory regime. Similarly, there is a difference between a service enforcing its own terms of service regarding minimum (or maximum) ages. In both these instances, the choice lies with the service provider. An interim position might be seen with age limits, should a regime require the service provider to enforce their own terms of service as regards age limits, where the service has chosen the age limits.

Lessons from the Australian Approach

12. The Australian model suggests[3] a restriction on access to a social media account. The requirement for a minimum age to have an account is not as extensive a prohibition as, for example, a shutdown of the internet or a total ban on smartphones would be. Under-age users still have access to other internet services and, since the prohibition relates to opening an account, means that under-age users can still view content from any social media platform that does not require an account to see (types of) content. It could be argued that this means the restriction is more proportionate from the perspective of freedom of expression – though to satisfy any rights assessment, any measure restricting freedom of expression must also be in the service of a legitimate

3 https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions/which-platforms-are-age-restricted

public interest and effective in achieving its goals. While the protection of children's wellbeing is undoubtedly a legitimate aim, does allowing access to non-account content (which could still be harmful content) undermine effectiveness? This illustrates the importance of getting the scope of any regulatory restriction right. It also emphasises the difficulty of relying on a single regulatory tool.

13. There are disadvantages to restricting access. It might be said that this approach reduces the pressure for services to aim for safe services, and that the corresponding shock to the user's system when they move from no social media to (unsafe) social media might be greater because the user will be moving into a comparatively much less safe space. This has been termed the "cliff edge" argument. Of course, the shock of a cliff edge would be less were the services to be effectively regulated - suggesting the need for regulation in addition to any access restrictions. A number of international organisations (e.g. UNESCO[4], Council of Europe Commissioner for Human Rights[5]) have emphasised the need for services to be safe by design.

14. Moreover, making the choice to exclude users below a certain age then means the price for safety is being paid by children, who have less access to products which may have benefits for them, rather than the company that designed the service and contributed to the problem.

15. This problem can be seen through the lens of human rights, though this point needs careful assessment. There is a clear potential for children's right to receive information and to express themselves to be adversely impacted should certain mechanisms for communication be restricted to them. It is not clear, however, the extent to which freedom of expression guarantees relate to access to a particular communication platform, rather than the right to speak on an available communication platform (subject to that platform's terms of service). The availability of other sorts of communications services could suggest that a restriction on one type of service was more proportionate in terms of its impact on the right.

16. A further consideration might be whether the services could ever be made safe enough for certain age-groups. It is accepted that some products are not available to children – tobacco, alcohol - but in these products the essential element of the product cannot be

[4] https://www.unicef.org/press-releases/age-restrictions-alone-wont-keep-children-safe-online

[5] https://www.coe.int/en/web/commissioner/-/regulate-platforms-not-children-council-of-europe-commissioner-for-human-rights-urges-caution-over-social-media-bans

made safe. Is social media in this category? This sort of question might suggest that a form of conditional ban - linking access to the market with safety standards - might be relevant.

17. Some commentators have noted that there is a concern about exclusion and "FOMO" when parents have imposed, on their own initiative, restrictions on their children's phone access/use. It might be argued that FOMO is less compelling if all young people are restricted, and justifies State action rather than relying on parental responsibility. The degree to which this argument is convincing is affected by (a) the services in scope and which services young people might adopt in lieu of open social media; and (b) the effectiveness of enforcement/ease of circumvention.

18. In terms of services in scope, the Australian model focused on social media platforms, excluding online gaming and messaging apps (the UK government consultation is seeking views on options for a wider scope, including those services)[6]. In terms of respecting children's rights to freedom of expression and freedom of association, this could be seen as a positive, but it does mean that a policy measure aimed at ensuring safety does not cover some services which have given rise to safety concerns. For example, researchers[7] have expressed concerns about child safety on Roblox; or concerns relating to group chats on WhatsApp. Children do not need to "circumvent" the ban, they can just go to services they already used that are not caught by the ban.

19. Furthermore, whilst some polling in the UK finds that support for a ban is high amongst parents, Public First found in their research[8] that the public do not think it will actually work. Indeed, 68% of UK adults surveyed agreed that a ban would not work in practice as children would find a way around it, e.g. by moving onto other platforms or through use of a VPN. 45% thought that a ban would push children onto less regulated or more harmful platforms. Parents are also unlikely to help with enforcement of a ban. Even if a ban was in place, 50% of parents said that they would likely still let their child access social media. This suggests that a ban would not eradicate the 'FOMO' argument set out above.

20. There is also the possibility that young people use VPNs to seek to evade the prohibition by trying to make it look like they are in another country. There were newspaper reports that VPN use in the UK surged when the children's duties and, specifically, the age

---

[6] **See Growing up in the Online World: a national consultation; pp32-3**

[7] https://think.revealingreality.co.uk/roblox-real-guide

[8] **https://publicfirsttech.substack.com/p/to-ban-or-not-to-ban**

verification obligation came into force in July. Ofcom's 2025 Review Report[9] notes that the number of UK VPN users had dropped again by October and recent research[10] from the Safer Internet Centre suggests that the summer surge was not due to children using VPNs. In terms of enforcement of the underlying rules, as the e-Safety Commissioner's Office has noted, it is possible that other signals might give away where a user is located; moreover, other industries use more effective location identification tools (e.g. gambling sector) – e.g. GPS data or mobile mast data. In some cases, the content of an account or the user sign up data may be a giveaway.

21. This, however, turns into a question of compliance and enforcement. It requires services to take steps beyond accepting location data based on IP address; it is uncertain whether the services would be proactive in that regard. It is also uncertain how much enthusiasm the regulator would have for broader enforcement responsibilities. Note that in the Australian model the obligation is for the service to take reasonable steps; they are not required to ensure 100% effectiveness. Where will the regulator draw the line on what is reasonable given the range of options open to service providers and given the state of age verification technology at the moment?

22. There are concerns about unintended consequences of a ban. For example, it has been suggested that the impact of these rules is to move interactions away from open platforms and on to encrypted services, which could make detection of problems more difficult, though as yet the evidence on this is not available. It might also be that young people are more hesitant to ask for help if they are on social media platforms illicitly.

23. Age verification can give rise to concerns about privacy and data protection. Most regulators seem to be aware of this; and many jurisdictions have data protection rules which seek to limit these concerns. Complying with one set of regulations (e.g. a requirement to restrict access) is not a justification for ignoring the data protection regime. Service providers should seek age assurance solutions that are privacy respecting. In this context, poor or malign compliance should not be treated as automatically indicating the regime is faulty; enforcement here whether by online safety regulator or data protection regulator is key.

---

9 https://www.ofcom.org.uk/about-ofcom/our-research/online-safety-in-2025-summary-of-the-technology-sectors-response-to-online-safety

10 https://saferinternet.org.uk/blog/new-research-from-childnet-into-vpns

24. The above discussion suggests that a ban, even if it is effective, is not a silver bullet and that an approach based on ensuring safer services backed up if necessary by a conditional ban might be a more optimal solution. This approach is backed by expert child safety and online safety groups[11], including many in the Online Safety Act Network. Recent polling by More in Common[12] found that amongst UK parents 67% would feel more positively towards a political party that supported increasing online safety protections. Furthermore, at the start of March, Girlguiding released research[13] that almost 7 out of 10 (69%) girls they surveyed said they would prefer to know if a platform is safe rather than an outright ban, and only 15% of 10-16 year olds think a social media ban will make them feel safer. Indeed, apart from what young people feel, we should note that a ban may stop children from seeing certain content, but it will do nothing to prevent the circulation of child sexual abuse material, or the generation of fake images using online text to image generators. Moreover, a ban will not address the business models, practice and products that continually prioritise profit over safety.

25. In this section, we put forward proposals to strengthen the Online Safety Act, which draws on the existing legislative framework to robustly regulate services and ensure that they are safe by design, in line with expected consumer protection standards as well as international human rights standards.

26. The Online Safety Act is long and complex but Parliament's intent when it passed was clear. It is set out in the very first section of the Act: "making the use of internet services regulated by this Act safer for individuals in the United Kingdom" with the duties imposed on providers intended to secure "among other things" that services regulated by the Act are "safe by design" and "operated in such a way that a higher standard of protection is provided for children than for adults".

27. Two years' on from the Act's Royal Assent, with the two main safety duties (on illegal harms and protection of children) now in force, it is unlikely that Parliament's expectations will be delivered any time soon. Partly this is because enforcement takes

---

[11] https://www.onlinesafetyact.net/analysis/under-16-social-media-bans-views-from-our-network

[12] https://www.moreincommon.org.uk/our-work/research/parents-talk-online-safety/

[13] https://www.girlguiding.org.uk/about-us/press-releases/social-media-companies-need-to-do-more-to-protect-young-people/

time. Crucially, however, Ofcom's narrow interpretation of a number of key provisions in the Act has led to it taking an overly cautious, risk-averse approach to drawing up the codes of practice for the two main safety duties. The regulator's interpretation of the Act does not reflect the intention that services be safe by design: an intention the former Secretary of State further emphasised in his Statement of Strategic Priorities for Online Safety.
[14]

28. The result is a gap between the risk assessment requirements and the mitigation obligations. While the risk assessment provisions require services to look at how the design of their service (including its business model) contribute to the risk of harm, Ofcom has included in its codes detailing the required approach to mitigation only, limited measures based mainly on ex-post interventions to reduce the impact of harm that has already occurred rather than upstream, content-neutral, "by-design" interventions to seek to prevent it occurring in the first place.

29. The key to this is to require safety by design. It should cover both the process (including governance mechanisms) and the end design. There is no one understanding of safety by design, but it can be seen to have three elements:
    1. that safety be considered throughout the lifecycle of the product from design, development, deployment, maintenance and de-commissioning or removal of features;
    2. A hierarchy of control approach (in line also with the UN Guiding Principle on Human Rights) whereby reduction of hazards is preferred to risk management of remaining hazards, with remediation being the mechanisms of last resort; and
    3. The consideration of safety through the entire value chain, with problems being tackled as close to source as possible.

30. Within this model product testing and red teaming are important, as are risk assessments more generally. Given the complexity of product design it is not to be expected that there will be easy or obvious solutions and there will always be some tradeoffs. There must be some degree of flexibility in how services approach these questions, and to take into account that safety is to some degree relative. As the Online Safety Act recognises, children are deserving of higher protection. Nonetheless, there comes a point where the question is, if a digital service or functionality cannot be made

[14] https://assets.publishing.service.gov.uk/media/6863b0e7b77395b48b609d86/Final_Statement_of_Strategic_Priorities_for_Online_Safety-_web_optimised.pdf

reasonably safe for its likely user base, should it be allowed on the market?

31. The Online Safety Act contains solid foundations. It would seem time efficient to build on these to remove some of the difficulties around effective enforcement and so to tackle these challenges.

32. The Online Safety Act Network has developed a package of proposed amendments aiming at ensuring that Ofcom uses its powers in the way that Parliament intended, holding companies to account for action to address all the risks that occur on their platforms, and reinforce the Act's underpinning objective to make products and services "safe by design" - for everyone. The plan would deliver a minimum standard of safety for all UK social media users but particularly children.

33. We draw the committee's attention to our 10 point plan for strengthening the Online Safety Act[15], which we see as the most effective way for ensuring all users, including children, are safe online.

Online Safety Act Network

March 2026

15 https://www.onlinesafetyact.net/documents/1189/OSA_Network__a_10-point_plan_for_Government.pdf