WRITTEN EVIDENCE FOR THE HOUSE OF LORDS COMMUNICATIONS AND DIGITAL COMMITTEE

The Online Safety Act: implementation and impact

September 2026

About CCIA

1. The Computer & Communications Industry Association is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For more than 50 years, CCIA has promoted open markets, open systems, and open networks. Its members include companies offering social media services, search engines, AI services, and related digital services in the UK.

Summary

2. CCIA understands the Committee's concern that the regime is not yet delivering everything Parliament intended.
3. At the same time, many companies large and small have faced an enormous pace of regulatory change, in many cases going beyond apparent legislative intent.
4. CCIA's submission seeks to reconcile these two apparently contradictory understandings of the process since the passage of the Online Safety Act.
5. Obligations are now arriving from multiple departments and regulators at once, faster than any one intervention can be assessed and reviewed. Some of these directly address concerns in Parliament and the wider public, but many are less relevant and reflect regulatory inertia, or old political priorities.
6. While companies can and have invested enormously in making online services safer, and responding to regulatory expectations, capacity (including in regulators and the government) is not infinite. There are not yet durable and workable mechanisms for correcting regulatory decisions that turn out to be wrong, which means mistakes continue to function as a barrier to new initiatives.
7. There is also a vital distinction that matters across the questions raised by the Committee: is the OSA being implemented and having an impact for more responsible and popular services; and is Ofcom finding it possible to enforce among the large number of long tail services that might be less able and/or willing to engage with the regulator.
8. Over time there is a risk that ad hoc political corrections become the norm, rather than an overall orderly online safety legislative framework. This would serve neither children nor the stability of the wider regime.
9. CCIA does not recommend reopening the Act's basic architecture. A risk-based approach remains the right one. The recommendations below are specific and broadly already within Parliament's remit.

Impact of the Online Safety Act

Question 1: What evidence is there that children are safer online since the protection of children duties came into force?

7. Ofcom's statutory report on the use of age assurance, published on 27 July 2026, provides a recent assessment of the regime's child safety requirements. It draws principally on the first six months after the duties of the OSA commenced. Its conclusion, that highly effective age checks work when implemented properly, is a finding about mechanisms rather than about outcomes for children, and Ofcom presents it as an early finding.
8. Care is also needed with the evidence base. Ofcom has relied heavily on survey data and self-reported exposure to harmful content, which is not a reliable indicator of exposure to the specific harms the Act defines. Comparable regimes elsewhere are at a similar stage, and the Australian restrictions, **which preceded the UK's under-16 proposals,** on which parts of the UK package are modelled have not yet generated longitudinal evidence either.
9. There are potentially two questions contained as part of this question, and they have different answers. Firstly, on the services that have brought in strong age checks, as Ofcom asked, are children actually safer? Secondly, how far has Ofcom got in making the rest do the same? There are tens of thousands of services, and some have little interest in complying, or refuse outright. These are different problems with different solutions. If children can no longer use a large, well-run service, some will move to smaller, less controlled ones, where they are less protected rather than more. The questions therefore need to be separated, both by type of harm and by whether a service is one that has acted or one that has not.
10. CIA suggests the Committee may find it more useful to look first to the evidence already in prospect, rather than to a new set of bespoke metrics that would be hard to collect and to compare across very different services. Two sources are well suited to this: Ofcom's own analysis of the risk assessments it has gathered from providers, including those released in response to freedom of information requests; and the transparency reports that categorised services will shortly be required to produce. Directing attention to these would give Parliament something concrete to assess as the regime matures, without pressing Ofcom toward prescriptive reporting demands.

Question 4: Have the Act's provisions been effective in driving services to identify risks, take proportionate action, and make meaningful changes?

12. Ofcom now holds risk assessment records from providers across the regulated population, gathered in the window ending 31 July 2026. Here the regulator holds the most comprehensive overview of whether services have identified risk and acted on it.
13. It may help to separate two key groups when assessing effectiveness. The larger, more established services already have sizable safety teams and the most responsible are drawing on those resources to take action that meets the Act's objectives and raises the bar across the industry.The harder test is the long tail of smaller services that took less action prior to the Act being in force, asking whether the Act got them to engage at all and more meaningfully. Ofcom holds the risk assessments that would answer both sets of questions.

Question 6: What unintended consequences have arisen from the Act or its implementation?

14. We draw the Committee's attention to three main areas.
15. The first concerns the cost of age assurance to users who are not the intended subject of protection. Ofcom's July report states that no single age assurance method or process eliminates the risk of circumvention. Demanding verification creates friction for adults reaching lawful content, but lighter verification is more easily bypassed. This does not imply that age checks are ineffective, however, but implies multiple 'lighter' checks working together over one heavy gate will often be more effective and less inconvenient for users. A single onerous check makes life difficult for ordinary adult users and can still be circumvented (including by using services that have not adopted age checks), whereas layered checks, as the Digital Trust and Safety Partnership recommends,[1] tend to work better. It also lets services collect less personal data, which matters for security as much as for user convenience. The most demanding checks tend to rely on sensitive identifiers, such as government issued documents or facial imagery, and concentrating that information makes any service holding it a more attractive target for cyber attacks. It minimises what is collected, through lighter and layered checks that establish age without amassing identity documents, is consistent with the data minimisation principle in UK data protection law and lowers the privacy and security risk to users of all ages.
16. The second is displacement. Restrictions applied to compliant services do not remove demand; they serve to redistribute it elsewhere in many cases. Research by Lang and others on age verification requirements found measurable shifts in search behaviour towards alternatives outside the regulated perimeter[2]. A regime that falls hardest on the services investing most in safety, while leaving those that are harder to reach in practice (e.g. because they have a minimal UK presence, or are generally small) can leave the children it is designed to protect at greater risk. These services are still covered by the law. The problem is that many are less able or less willing to follow it, and therefore acting against them takes longer with IP blocking rightly a last resort.
17. The third concerns the effect on services at the margins of the regime. The Act reaches well over 100,000 services, the majority of them operated by small businesses, charities, and volunteer communities. For a service of that size, the cost of working out what the Act requires of it, from risk assessments to whether it is in scope and which category it falls into, and of challenging those decisions where necessary , can exceed the cost of leaving the UK market. If a service pulls out, the people who used and valued it bear the cost.

Ofcom's implementation and enforcement

Question 10: Are there factors limiting Ofcom's ability to carry out its duties effectively?

18. Three, in CCIA's assessment.

[1] Digital Trust & Safety Partnership, 'Age Assurance: Guiding Principles and Best Practices' (September 2023) https://dtspartnership.org/age-assurance-guiding-principles-best-practices/
[2] David Lang and others, 'Age Verification and Public Adaptation: A Pre-Registered Synthetic Control Multiverse' (2026), https://journals.sagepub.com/doi/10.1177/2755323X251415424.

19. **The accumulation of regulatory requirements.** A change to a digital service now has to satisfy Ofcom under the Act, the Competition and Markets Authority under the Digital Markets, Competition and Consumers Act, the Information Commissioner on data, the Home Office on access to data, and the Competition Appeal Tribunal in the event of collective proceedings, among many others. CCIA set this out in its response to the Lords Industry and Regulators Committee in January 2026 as analogous to the tragedy of the anticommons described by Heller:[3] many bodies can halt a change unilaterally and none can approve one. The cumulative effect exceeds what policymakers intended in any single area, and it constrains Ofcom as much as anyone, because Ofcom cannot resolve requirements that sit outside its remit. The Digital Regulation Cooperation Forum exists to coordinate several of these regulators; giving it a clearer and more transparent role in reconciling overlapping requirements would help to contain the problem.
20. **Capacity.** While companies can and have invested enormously in making online services safer, and responding to regulatory expectations, capacity (including in regulators and the government) is not infinite. In the twelve to eighteen months from mid 2026 it is expected to deliver, among other things, codes of practice relevant to Category 1, 2A, and 2B services; the response to the additional safety measures consultation and the resulting code amendments; the statutory report on content harmful to children; the report on app store harms; the first Online Information Advisory Committee report; the fees regime; the first regulations arising from the Government's under-16 announcements; and the transparency reporting cycle. Each can be justified on its own but together they represent a significant amount of concurrent change that will absorb many of the same specialists who would otherwise be responding to new emerging risks. There are practical decisions to be made about prioritisation here: effort directed at activities with little direct relevance to user safety (e.g. creating large ad repositories) or which outright make creating safe services harder (e.g. restrictions on personalisation) is effort not directed towards addressing the priorities of Ministers, Parliamentarians and users.
21. Thirdly, we are concerned by the **absence of a workable correction mechanism** for when the regime produces outcomes that were not intended. The Act gives Ofcom the power to strike significant balances between freedom of expression, protection of children, and privacy, with substantial economic consequences attached to decisions such as categorisation. Regulators exercising powers of that kind can make mistakes, as all institutions do. What matters is whether mistakes can be corrected.
22. The recent categorisation litigation illustrates this difficulty. The Wikimedia Foundation, a charity, challenged the Category 1 threshold conditions. The High Court dismissed the claim in August 2025, while observing that the judgment did not give a green light to a regime that would significantly impede Wikipedia's operations, and indicating that the Secretary of State might be obliged to consider amending the regulations or exempting categories of service. Almost a year later, in July 2026, Ofcom notified the Foundation that Wikipedia is not currently a Category 1 service but will remain on a watch list of services that could be designated in future. The Foundation therefore obtained a

[3] Michael Heller, The Tragedy of the Anticommons: Property in the Transition from Marx to Markets, https://repository.law.umich.edu/cgi/viewcontent.cgi?params=/context/articles/article/1608/&path_info=111HarvLRev621.pdf

discretionary reprieve rather than prompting a change of approach which would have had wider benefit, after a year of litigation that few organisations of its size could contemplate.

23. The consequence of this will be cumulative. Errors that cannot be corrected do not fade but rather they compound, and the pressure they can generate is political as much as legal. External merits-based review would be a necessary stabiliser for a highly complex regime.

Adequacy and future of the legislative framework

Question 11: What specific changes are needed to the existing provisions?

25. CCIA recommends three changes.
26. **Review and prioritise requirements.** Ofcom should be required to streamline and review requirements with relevance to user harms, e.g. requirements for an advert repository, and ensure it focuses on higher priority interventions.
27. **A route to merits review (a proper second look at whether the decision was right, not just whether it was made lawfully), or an equivalent mechanism, for substantive decisions under the Act.** This is the recommendation CCIA made to the Lords Industry and Regulators Committee in the context of regulators and growth, and it applies with particular force here given the breadth of the judgments the Act asks Ofcom to make. The purpose is to allow errors to be corrected without recourse to judicial review, which tests the lawfulness of how a decision was taken rather than its substance and is available in practice only to those who can fund it. A merits review is usually quicker too. Under judicial review the court can only send the decision back to Ofcom to take again, whereas a merits review lets the tribunal put the mistake right itself. Linklaters found the same in a study of appeals against Digital Markets Unit decisions.
28. **Risk-based regulation of categorised services rather than blanket categories.** The current conditions do not reliably distinguish the high-risk services the duties were designed for from low-risk services that happen to meet a quantitative or feature-based test.

Question 12: Beyond amending the Act, what action should be taken?

29. Following the July 2026 dissolution of the Department for Science, Innovation and Technology and the distribution of its functions, responsibility for online safety, for AI policy, and for data protection now sits across multiple departments, and the position on some functions has not been comprehensively set out at the time of writing. A published statement of which department leads on which element of the online safety framework, and a single sequencing plan covering the Act's remaining implementation alongside the measures announced in June and July 2026, would ensure clarity and give both Ofcom and regulated services a stable planning horizon.

Question 13: How well can the framework respond to emerging harms and technologies?

30. The Act's duties are drafted in terms of systems and processes rather than named technologies, and that generality has so far allowed the framework to reach services

that did not exist when it was drafted. CCIA does not consider that further primary legislation is required to bring emerging technologies within scope.

31. The constraint is the speed at which guidance can be produced and absorbed, and here the earlier discussion in the answer to question 10 is relevant.

Question 14: What impact could recent and proposed additions to the framework have on the Act's implementation and effectiveness?

32. A substantial body of new policy has been introduced alongside the Act within a matter of months. The Government's June 2026 progress statement proposed to prevent social media services being offered to users under the age of 16 and its July 2026 response, and the accompanying Written Ministerial Statement of 15 July, confirmed that approach and went considerably further with default restrictions for 16 and 17 year olds, including an overnight curfew and the disabling of autoplay, personalised feeds, live streaming, and contact from strangers; mandatory breaks for under 18s using AI chatbots, with the option of restricting services that pose a risk to them; a new duty on services to detect and prevent attempts to circumvent these rules; and a request that Ofcom report by October 2026 on age assurance capable of establishing whether a user is over 16. A number of these measures are being taken forward through the Children's Wellbeing and Schools Act 2026 rather than through the Online Safety Act. The regime a UK user actually encounters is the compound of all of these measures, and the coherence problems they create appear only when they are assessed together.
33. The interaction with the Act's own provisions is where some difficulty will lie. To take the clearest example, the request that Ofcom report by October 2026 on age assurance for the over 16 threshold runs in parallel with Ofcom's existing statutory work on age assurance under the Act, which is due to report in the same period, with two parallel workstreams on the same question, applied to the same services. The default feature restrictions for 16 and 17 year olds overlap the children's safety duties that services are already implementing under the Act, and the chatbot measures regulate providers that are, in many cases, already within the Act's scope, but through a separate mechanism. We would encourage the Committee to recommend that each addition to the framework be tested for coherence with the Act before it is introduced, and that the several measures be assessed as a whole rather than one at a time.
34. Several key aspects relating to chatbot use by under 18s remain undefined. On the Government's own account, the following are unsettled: the frequency and duration of mandatory breaks, referred to an expert panel; the definition of the intimate functionalities to be restricted, which was stated more widely in June than in July and has not been reconciled; the standard for harmful, inaccurate, or unverified mental health advice; and the scope of the business and customer service exemption. Providers are being asked to plan against parameters that will be set after the commitment to legislate has been made. These are matters that a thorough Ofcom consultation on draft codes, drawing on third-party evidence, is best placed to resolve. They should be worked out through that process, and compliance judged only once it has, rather than settled in advance.

35. These uncertainties matter for the coherence of the wider framework, and CCIA will address them in full in a forthcoming paper on the Government's chatbot proposals. Two points are particularly important here. The measures are aimed at a narrow harm, the emotional attachment that can form through services designed to simulate a relationship, but as drafted they reach every chatbot a young person uses, from general purpose assistants and accessibility tools to the workplace software used by apprentices and agentic products that run tasks in the background. Secondly, a fixed timer-based break cannot distinguish revision from reflection, or a homework session from a safeguarding disclosure, so it risks interrupting the interactions that matter most while doing little about the narrow category of service the evidence actually concerns. Both problems trace to one question the measures currently leave open, whether a chatbot is defined by its interface or by its purpose. Reserving the most restrictive requirements for the services the evidence supports, would protect children more effectively than rules applied uniformly to tools that carry very different risks.
36. On the sequencing of the circumvention evidence, Ofcom's research and report on circumvention is not expected until spring 2028, after the chatbot regulations are anticipated to be made. Circumvention is the question that determines whether any of these measures bind. Establishing the answer before the rules are drafted, rather than after, would allow it to shape the design.
37. **Interaction with the Act.** The Government has said the new measures layer on top of the Act rather than replacing any part of it. Where the same service is subject to children's duties under the Act and to separate statutory restrictions on the same users, with age assurance expectations set through two processes at two thresholds, the risk is not that services face too much regulation but that they face inconsistent regulation and cannot comply with both. The Act already has a standard for this, the "highly effective age assurance" test Ofcom uses. Using that same test for any new measures, instead of inventing a second one, would provide greater clarity.

Oral evidence

41. CCIA would welcome the opportunity to give oral evidence to the Committee, and would be glad to provide further detail on any of the above in writing.