



## REQUIREMENTS FOR CODE MEASURES - TECHNICAL FEASIBILITY AND PROPORTIONALITY

---

### Introduction

1. Ofcom has obligations to develop codes to assist regulated service providers fulfil their safety duties (s 41 OSA). Services which comply with the codes enjoy a “safe harbour” in that they are deemed to have fulfilled their safety duties under the Act (s 49(1) OSA). Schedule 4 sets down requirements around the nature of any measures Ofcom decides to include in a code.
2. This paper considers what those requirements mean as there has been some concern that some interpretations of these conditions, specifically that of technical feasibility, might lead to the situation where “rather than taking proactive steps to safeguard users, [services] simply opt out of finding innovative solutions to prevent harm”<sup>1</sup>, especially given the safe harbour provisions. This issue first came into view when the Illegal Content Codes were revised from the version set down for consultation to the final published version by the inclusion of references to technical feasibility in relation to some measures.<sup>2</sup> The issue returns again in the consultation on [additional safety measures \(ASM\)](#).
3. We discuss:
  - The relevant provisions in the Act
  - The different considerations these bring into play
  - Commentary on Ofcom’s interpretation of “technically feasible” in its codes measures
  - Recommendations to address the risks to the mitigation of harm arising from these issues.

---

<sup>1</sup> Gregor Poynton MP, Debate on Online Safety Act: Implementation, 26 February 2025, Hansard (HC) Vol 762, Col 393WH,

<https://hansard.parliament.uk/Commons/2025-02-26/debates/00959567-3EC5-4AF6-94DC-A242D0EE1B0A/OnlineSafetyActImplementation?highlight=%22technically%20feasible%22>

<sup>2</sup> See our response to the final codes here:

<https://www.onlinesafetyact.net/documents/168/osa-network-illegal-harms-response-final.pdf>; and reporting on children’s charities’ concerns here:

<https://www.standard.co.uk/business/business-news/children-will-be-left-exposed-to-sexual-abuse-online-under-current-safety-rules-b1211727.html>

## The Nature of the Requirements

4. The relevant provisions are found in [Schedule 4](#) to the Online Safety Act, at para 2 and – in addition to provisions relating to detail and clarity - read as follows:

(c) the measures described in the code of practice must be proportionate and technically feasible: measures that are proportionate or technically feasible for providers of a certain size or capacity, or for services of a certain kind or size, may not be proportionate or technically feasible for providers of a different size or capacity or for services of a different kind or size;

(d) the measures described in the code of practice that apply in relation to Part 3 services of various kinds and sizes must be proportionate to OFCOM's assessment (under section 98) of the risk of harm presented by services of that kind or size.

Other requirements, for example those as to privacy, also apply but are not discussed here.

5. While both Jeremy Wright<sup>3</sup> and Baroness Jones<sup>4</sup> implicitly suggest that technical feasibility and proportionality are one thing, and Ofcom links proportionality and technical feasibility together in its ASM consultation (para 1.22), it could be said that there might be a number of different aspects in play:
  - 1) that the measure prescribed is possible at all;
  - 2) that the measure is feasible in relation to a particular class of services/providers;
  - 3) that the measure is proportionate.
6. These are considerations Ofcom must be satisfied about before it introduces a measure into a code in relation to all relevant services or an identified sub-set of them.

## How do we distinguish between these considerations?

*Is it possible?*

7. The first aspect seems to be an objective test, irrespective of the nature of any particular service. It requires that the measure be possible at least in some circumstances. It avoids the possibility that Ofcom might ask for the impossible – the digital equivalent of requiring that the laws of gravity be suspended. Ofcom notes some sorts of activities are “technically challenging”, such as

---

<sup>3</sup> Sir Jeremy Wright, MP , Debate on Online Safety Act: Implementation, 26 February 2025, Hansard (HC) Vol 762, Col 387WH,

<https://hansard.parliament.uk/Commons/2025-02-26/debates/00959567-3EC5-4AF6-94DC-A242D0EE1B0A/OnlineSafetyActImplementation?highlight=%22technically%20feasible%22>

<sup>4</sup> Baroness Jones, Debate on Online Safety Act 2023 (Category 1, Category 2A and Category 2B Threshold Conditions) Regulations 2025, Hansard (HL) Vol 843, Col 1544,

[https://hansard.parliament.uk/Lords/2025-02-24/debates/28261053-381E-4A43-924E-7BCD107C45DB/OnlineSafetyAct2023\(Category1Category2AAndCategory2BThresholdConditions\)Regulations2025?highlight=%22technically%20feasible%22](https://hansard.parliament.uk/Lords/2025-02-24/debates/28261053-381E-4A43-924E-7BCD107C45DB/OnlineSafetyAct2023(Category1Category2AAndCategory2BThresholdConditions)Regulations2025?highlight=%22technically%20feasible%22)

the deployment of scalable solutions to moderate livestreams in realtime (see ASM consultation para 6.3) This is presumably different from saying that something is infeasible.

8. One issue that is not directly recognised by the wording in the Act is that some things might vary depending on tools and techniques provided by third-party providers. This is a form of contextual infeasibility in that it might be nothing to do with the service provider itself, so has similarities to objective infeasibility in that there might be nothing the regulated service can do. It may be that this form of infeasibility is best dealt with by an obligation to take steps to deal with the issues, accepting that those steps might not be effective in all cases (as noted for example in the ASM consultation para 6.29).

*Is it feasible in relation to particular services or providers?*

9. The second aspect recognises that not all services have the same features. For example, requiring image-based analysis on a text-based platform would not seem feasible – this would seem to map on to para 2(c)'s reference to different kinds of service. End-to-end encryption -depending on how it is implemented - blinds services to what their users are doing, so some content-based measures might not be feasible (see eg hash-matching obligations for intimate image abuse, ASM Consultation para 11.13 and terrorism content, ASM Consultation para 12.11). The capability of the service to implement the measure would not be there. It is noteworthy that this could cut across even an obligation imposed by the text of the Act on all user-to-user services; that is, the requirement in section 10 OSA that a regulated service must have a system in place to remove content swiftly once on notice of that content (this limitation is restated by Ofcom in its ASM consultation at para 5.10). It might even be that some measures are dependent on there being a certain number of users (eg using data analytics). This aspect of the requirement is therefore relative to types of service.
10. There must surely be, however, a limit to the possibility of a service avoiding obligations by saying that they do not do that and therefore do not have the capacity. For example, were Ofcom to seek to impose an obligation to retain certain sorts of information, would it be acceptable for a company to say that that obligation was not technically feasible because the service provider did not currently have the systems in place to gather and store data? Certainly, in relation to the obligations for recommender systems in the ASM consultations, when discussing the availability of “relevant information” for determining if content is potentially illegal, Ofcom states that, “... recommender systems should then be designed and operated in a way to take appropriate account of that information, and to exclude content indicated potentially to be illegal content from users' recommender feeds”. This suggests that some changes to systems may be required (para 14.21, see also 14.22-23). Nonetheless, it is unclear where Ofcom will draw the line in practice.

*Is it proportionate?*

11. The third aspect to be taken into account is proportionality. Proportionality can be seen as proportionate to type of harm, or likelihood of a harm arising, or by reference to the costs not just against the background of the severity of harm but also the resources of the provider itself.

It could be that this economic aspect of proportionality is dealt with by paragraph 2(c) with the harms aspect of proportionality dealt with separately in paragraph 2(d). Certainly, it could be argued that the boundary between economic proportionality considerations and relative feasibility considerations might in some instances start to blur into one another (and may be why they are sometimes referred to together). It seems better, however, in terms of drawing clear boundaries to distinguish between the situation when there is a functional issue and the situation where a technical or functional solution is available but is expensive. The latter is best dealt with as (economic) proportionality. This issue of proportionality of cost (and proportionality bearing in mind severity of harm) arise more generally throughout Ofcom's analysis.

## Commentary

12. It is noticeable that Ofcom has chosen to insert the phrase “where technically feasible” in some measures rather than assessing the issue for themselves. It could be said that the Act provides that these requirements are considerations to be applied ex ante (before the rule goes in) rather than a justification for non-compliance ex post. Indeed, in some instances Ofcom has assessed the measure to be technically feasible – see eg ASM Consultation para 5.40 and 16.24 – suggesting that this sort of determination is possible.
13. A consequence of including proviso wording in the measure is that this has the effect of allowing the service providers – at least in the first instance – to determine whether they need to comply with the measure or not. While Ofcom will ultimately be able to determine the appropriateness of that decision in a given case, a key concern is the approach of Ofcom to monitoring self-declared technical infeasibility. What standards will it apply and how will it factor in financial considerations (over and above the financial considerations it has already taken into account for the proportionality analysis of the measures in its consultations)? There is also a question of when: how long will it take Ofcom to identify if a provider has relied on technical measures as well – what is Ofcom's process for finding out and how long will it take?
14. Another consequence of incorporating the technical feasibility as proviso language is that the service provider will satisfy the measure (at least on its own assessment) and therefore benefit from safe harbour; it does not seem that such a service provider would be under any obligations to take other remediation steps. There is no expectation from Ofcom that they might need to expand their implementation of other measures to fill any gap in protections as a result of it being, on their assessment, “technically infeasible” to implement the one at issue. Nor is there any determination as to how long a service can have this safe harbour: shouldn't the service provider have to demonstrate on a regular basis that it is looking to overcome the technical limitations and fully comply with the measure? This has implications for progress in online safety solutions across the board: indeed, concerns have been raised previously – not just by civil society but also by the safety tech sector - about the impact of low standards in codes in combination with the safe harbour and the fact that they disincentivise innovation in the online safety sector.

15. As well as potentially preserving the current “technically feasible” status quo indefinitely, this means that even obligations which are set out on the face of the Act – notably the obligation to have a system to take down illegal content swiftly once on notice – could be weakened or undermined; the limitations here could have an impact on the effectiveness of other measures (eg crisis response protocol – see discussion of interaction with take down system: ASM consultation para 20.20). This tension lies in the drafting of the Act, though Ofcom could mitigate this position by imposing obligations on companies to take alternative measures (eg account level actions in relation to concerns about content – see e.g user banning in response to CSAEM, or measures to introduce safety defaults for child users (Measures ICU F1 and F2)).
16. It is submitted that in determining the boundary of, in particular, relative technical infeasibility, Ofcom should adopt a high threshold – not least because otherwise there is a greater risk that services would not be safe by design (and that is the objective of the regime as identified in s 1(3) OSA). There are other mechanisms by which the problem of technical considerations can be resolved. For example, the obligation in relation to third-party tools could be to take steps to prevent screen shots, but not to require that the attempt be 100% successful. Ofcom has taken this approach in relation to user banning and prevention of return following detection of CSAEM (measure ICU H3). In other circumstances, where services are of the opinion that because of the specificities of their respective services, they cannot take the measures envisaged, they could address the concern by other means – a possibility envisaged by the Act to allow for the individual circumstances of specific providers. This has the advantage of avoiding the safe harbour loophole noted.
17. Tightly defining the scope of technical feasibility also reduces the risk of another concern: that services make design choices to take themselves outside the regulatory obligations which have become technically infeasible. While changes to a service to achieve this would presumably be picked up by a risk assessment, it is not clear if Ofcom feels it has the power to stop a service implementing such changes (what it expects services to do is set out/limited by the Codes). A narrow focus for the technical infeasibility opportunity reduces the incentives for this – but this must be clear to service providers in advance.

## **Recommendations**

18. On the basis of the above – and given the significant concerns about the impact of this, particularly in relation to CSAM and other illegal harms – we would suggest the following:

### *Legislative amendments*

- Ofcom is constrained by the Act, but the interplay between the “technically feasible” provisions and requirements for “proportionality” create confusion and are not clearly defined. We would suggest that the Government amend the Act so that the language relating to “technically feasible” is disaggregated from resources and proportionality in Schedule 4, para 2(c) to ensure that, when it comes to Ofcom’s drafting of codes of practice, this distinction is clear.
- The Act could also be amended to require service providers to notify Ofcom if they are relying on the “technically feasible” proviso so that the regulator can then scrutinise this decision.

- The Government also needs to remove the “safe harbour” provision relating to the Codes – as we and others have argued frequently in relation to the impact it has on setting a low bar for compliance with the Act’s duties. Or, alternatively, that Ofcom needs to require alternative measures from companies who say that a specific code measure is not technically feasible to bring this more into line with the “comply or explain” expectation within the Act.
- A further legislative consideration to prevent the deliberate rollback of protections and standards might be the requirement that, should a service redesign its features or functionality to make their compliance with a measure not “technically feasible”, this should trigger a further risk assessment along with the compensatory measures suggested above.

#### *Ofcom’s approach to code measures*

- The “technically feasible” proviso is used in different ways in relation to different measures. Ofcom needs to ensure, in its final version of the additional safety measures, that the application of this proviso is consistent and should provide additional commentary on this in its final statement. We have suggested above that the proviso should only be included in measures in more limited circumstances and that for other types of technical infeasibility other solutions should be adopted. The regulator also needs to publish a stronger clarification of where the boundary between “technically infeasible” and “too costly to implement” lies for services of different sizes.
- Technical capability moves at a fast pace, but there is no timescale set out for Ofcom to review when the “technically feasible” proviso might no longer be relevant for services who have exercised it. Ofcom needs to set out the process for reviewing advances in technology that make this proviso redundant and commit to revising the relevant codes measures with an expectation that this be done within 9 months of that determination being made.
- Where Ofcom can justify that the “technically feasible” proviso is justified, it should make clear that service providers who rely on this in their approach to compliance will be expected to demonstrate that they have assessed which other measures can be more robustly or expansively implemented to reduce the risk of harm to which users are exposed as a result of their inability to implement the “technically infeasible” measure.

#### *Ofcom’s approach to enforcement*

- It is not clear how Ofcom intends to assess which services are using the “technically feasible” proviso when complying with the code measures or whether their claims as such are evidenced. Ofcom need to publish a statement on how they will determine which these services are, and how they will assess whether the “technically infeasible” status is accurate and give some idea as to the standard that services would be expected to meet – to make it clear that “technically infeasible” applies to significantly more than inconvenience or extra costs.
- Ofcom also needs a process – as part of their monitoring and enforcement programme – to assess whether services are rolling back functionality in order to claim that a measure is therefore technically infeasible and set out the enforcement measures that they will take if such a rollback is identified. This is in addition to our proposal – which is necessarily on a longer time-frame – to amend the Act to trigger a new risk assessment in these circumstances.