Baroness Jones
Parliamentary Under-Secretary for the Future Digital Economy and Online Safety
Department of Science, Innovation and Technology
100 Parliament Street
London
SW1A 2BQ

14 February 2025

Dear Baroness Jones

FOLLOW UP TO CIVIL SOCIETY ROUNDTABLE - 12 FEBRUARY 2025

Thank you for hosting the discussion on the Online Safety Act at DSIT earlier this week and for your update on upcoming implementation milestones and the work underway in Government. We appreciated your willingness to listen to our concerns and the strong message you gave in your opening remarks about the importance of making the regime work and, as you said, “getting on the front foot”. You also spoke to the importance of the “messaging”, and we agree that communicating these efforts well is vital.

In our individual responses, we recommended a number of practical actions that the Government might take in this regard, to resolve some of the problems we see with both the Act and its implementation. Given the number of organisations around the table, you were - as you observed - left with a “long shopping list”. This reflects the fact that - as Lucy Powell MP said, speaking on behalf of Keir Starmer's office in 2023 - new legislation and a strategic reset is needed. The new government is implementing the regime of the previous government, little changed despite the criticisms made by the Front Bench in Opposition.

We therefore committed to writing to you to bring together the key, targeted interventions we recommended so that you and your officials might be able to consider them in more detail before responding. They are attached to the annex of this letter; a number of them have been shared previously with you and officials, for example in our letter to the Secretary of State about Meta’s changes to its content policies, to which we have not had a response. A detailed follow-up discussion on these, perhaps with more time available, would be welcome. In particular, we would be interested in your reflections on whether these specific suggestions are already covered by activities either the Government or Ofcom are already taking and, if not, whether they might be progressed urgently.

From our perspective, these are the bare minimum required to make the online safety regime work as Parliament intended when passing it. You rightly said that the current Government

“inherited” this Act. It is far from perfect but it is within your gift to improve it. In doing so, you will be able to deliver many of the objectives that your colleagues argued so strongly for in Opposition but which will not currently be realised by the Act - or by Ofcom’s interpretation of it. We fully appreciate the concerns you expressed at the end of the meeting about how difficult it is to get new legislation into the Parliamentary programme. However, these are small, technical amendments to the OSA that do not add significant new provisions to the Act, nor unpick the framework that already exists. Such “tidying up” amendments are part and parcel of bedding in a complex and novel legislative framework and should be seen as business as usual for the Department in delivering its responsibilities.

New legislation - and the necessary policy development and consultation to deliver that - will undoubtedly be needed before long. We mentioned areas including: suicide and self harm; the impact of fluid ideologies online and how, for example, an online environment of radical ideology and misogyny played into the murders in Southport; the need for an alternative dispute resolution mechanism; actions flowing from the pornography review; and AI-generated CSAM. We see no reason why the Government should not start planning for that now, as it will not interfere with Ofcom’s implementation plans or their first year of enforcement.

But, as you gathered from our discussion, our primary focus is on what can be done urgently to mitigate against the very real risk that Ofcom’s implementation and enforcement of the OSA “as is” will not live up to the expectations of Government or Parliament, nor will it deliver the step change in online safety that the British public, particularly parents, children and vulnerable groups, have been led to expect by both your Government and its predecessor.

It does not feel to us to be prudent to wait for that to play out. Our list of amendments in the annex is the first step towards mitigating that risk. Civil society resources are significantly stretched and, while requests from Government and Ofcom to respond to consultations and attend meetings are welcome, the outcomes rarely lead to significant changes to the direction of travel and often feel like they are tick-box engagement exercises. The failure of the Government to get to grips with Ofcom’s lack of ambition is creating avoidable burdens for civil society and, indeed, frustrations for DSIT, itself - for example, the recent parallel consultations on the data access provision - and our continued good faith engagement should not be taken for granted.

So - in the spirit of the constructive engagement that you asked from us - we hope that you agree that your officials should invest time in considering these proposals in detail in the coming weeks and that, in tandem, you will work with your Ministerial colleagues to identify suitable legislative vehicles to bring such amendments forward.

We look forward to hearing your initial response soon and stand ready to work with your team on the details of these; a standing monthly meeting to aid collaboration and review progress might assist both sides in this regard.

SENT BY THE OSA NETWORK ON BEHALF OF THE 13 ROUNDTABLE PARTICIPANTS

ANNEX: Proposed technical amendments to the OSA 2023

1. Introduce a general obligation on services to take reasonable steps to mitigate all the risks identified in their risk assessment. (See our letter to the DSIT SofS of 24/1 re Meta's policy changes)

2. Introduce minimum standards of terms of service for category 1 social media and search, e.g. for Equality Act protected characteristics, to provide a baseline of protections for users in the UK. (See our letter to the DSIT SofS of 24/1)

3. Insert a "no rolling back" clause to maintain ToS protections for users in the UK as they were at Royal Assent. (See our letter to the DSIT SofS of 24/1)

4. Introduce a requirement for Ofcom to produce a code of practice on safety by design, to deliver the objective set out in section 1 (3) and to focus more on harm caused by features and functionalities. This would underpin the existing, largely content-focused codes.

5. Remove the requirement in Schedule 4 for measures to be "clear and detailed", which is contributing to Ofcom's high evidential threshold and limiting the scope of the codes.

6. Remove the "safe harbour" provisions relating to the code of practice (section 49(1)) which means that companies can be in compliance with their safety duties without addressing all the risks they have identified on their service.

7. Upgrade the VAWG guidance to a code of practice to make it enforceable.

8. Amend the categorisation regulations to ensure the intent of the Act - that category 1 includes small, risky platforms - is delivered.

9. Review the list of priority offences to ensure that self-harm offences have parity with suicide.

10. Clarify the position on private messaging and end-to-end encryption, to ensure there are no safe havens for illegal content, such as child sexual abuse material

11. Set a minimum age limit for children's access and tighten up the wording in the Act around the requirement for providers to deliver age-appropriate experiences for children to ensure Ofcom delivers measures to bring this into force.

Additional legislative amendments

12. Strengthen the researcher access to data provisions in the Data (Use and Access) Bill

13. Strengthen the NCII Offence introduced in the Data (Use and Access) Bill to ensure recourse and/or civil redress for individuals; and make NCII content illegal.