Reset.

Evidence to Online Safety Bill Committee

Key amendment areas

Transparency

As drafted, the Bill requires platforms to document how it complies with the regulations, but this documentation is not made publicly available. In most instances, it is not even made available to Ofcom unless Ofcom initiates an investigation. For example, the risk assessment duties require services to assess for and document a wide range of risks across their service, but these documents remain hidden inside the company. There has to be **greater transparency by <u>default</u>** if services are to be truly accountable.

- Cat 1 and 2A companies should have to publish their risk assessments to Ofcom at the very least - ideally they'd be made publicly available
- Cat 1 and 2A transparency reports should also be made publicly available rather than just submitted to Ofcom
    -

Access to data (cl 136)

At present, companies decide who accesses data, how much of it and for what purposes. Only the companies themselves can see the full picture, and the effect of this opacity is that it has taken years to build up the case for the Online Safety Bill. Without a greater level of insight enabling policymaking, quality research and harm analysis, regulatory innovation will stagnate.

It is abundantly clear that greater access and availability of data and information about systems and processes would improve the understanding of the online environment. We cannot rely solely on OFCOM to act once problems arise when new issues can be spotted early by experts found elsewhere.

Increasingly, researchers who need access to this information and data are not only based at academic institutions, but also within civil society organisations. Civil society plays a crucial role in identifying harmful content and poor behaviour, as work by the NSPCC, CCDH, ISD, Glitch and numerous other organisations prove.

These and other groups currently achieve this with access to minimal information and ongoing difficulties. Access to publicly available information from online platforms is routinely curtailed, often invoking the protection of users.

- Clause 136 requires that Ofcom publish a report on access to data in two years. This is too long.
- Ofcom should be required to ask how access to data should be achieved, not if it should be. And they should have to do so at an accelerated pace.

Content of democratic importance (cl 15)

The layers of free speech protections in the Bill make the Bill confusing and hard to implement. A Bill that's hard to implement will do nothing for online safety, nor for free speech.

Clause 15 is particularly high risk as it leaves platforms to determine what content of democratic importance really is. It also opens the floodgates for bad actors to promote harmful content on the basis of its democratic importance. COVID disinformation and false narratives about the fabric of the United Kingdom are two such examples. The clause also risks legitimising hate targeted at people in public and political life.

If the aim is to protect political engagement online, it would be better to delete this clause and instead insert the language from 15.3 into Clause 19. This has the same effect but reduces the complexity of the regime, while better protecting free speech.

- Delete clause and insert 15.3 into clause 19.

Bad actors - what does the Bill do?

The Bill is silent on coordinated inauthentic behaviour, which it risks encouraging via areas such as clause 15 and the media exemption. Any loopholes will be ripe for exploitation by bad actors bent on distributing harmful content.

The EU's Digital Services Act includes measures to account for how service design - including through manipulation- can have serious effects on mental health and wellbeing. This explicitly references coordinated disinformation campaigns.

- In the Risk Assessment duties (illegal; harmful to children; harmful to adults) explicitly require platforms to account for the risks of coordinated inauthentic behaviour.

Media exemption

Grave concerns about how this can be exploited by bad actors, as we are already seeing play out in the UK and more widely in the Rus/Ukr conflict. 49.10.b.iii would extend the exemption to UGC which includes links to recognised news publisher content. This is a tactic which is already being manipulated at scale to spread falsehoods online.

The proposal of an amendment which takes the exemption even further, creating a must carry obligation, is a free pass for disinformation and hate. Such a duty must not be included in the Bill.

- Narrow the definition of recognised news publisher in Cl 50.
- Clause 49.10.b.iii must be deleted

Safety by design

The best way to reduce harm while protecting free speech is to focus on safety by design. The Bill could go further in this regard.

For example, the DSA states that:

very large online platforms and very large online search engines should assess the systemic risks stemming from the design, functioning and use of their service, as well as from potential misuses by the recipients of the service, and should take appropriate mitigating measures in observance of fundamental rights.

It also calls for platforms *to mitigate the negative effects of personalised recommender systems* and t*o adjust recommender systems that "lead to the discrimination of persons in vulnerable situations".* These are the sorts of measures that should be included in the OSB.

- Include clearer safety by design metrics as per the DS