Your response

Volume 2: The causes and impacts of online harm

Ofcom’s Register of Risks

Question 1:	
i)	Do you have any comments on Ofcom’s assessment of the causes and impacts of online harms?
The Register of Risks provides an excellent assessment of the causes and impacts of online harms, and a good basis for a first set of codes. We would expect it to require regular updating as technology changes and evidence emerges, including as Ofcom exercises its information gathering powers under the Act, which we would encourage Ofcom to do soon and regularly.	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No	

Volume 4: What should services do to mitigate the risk of online harms

Our approach to the Illegal content Codes of Practice

Question 12:	
i)	Do you have any comments on our overarching approach to developing our illegal content Codes of Practice?
Ofcom’s approach has produced a very limited set of proposals, and risks falling a long way short of addressing the causes and impacts of harms identified in the Register of Risks. We are concerned that the gaps are so large and numerous that the Codes may even fall short of delivering the stated aim of the Act as set out in Section 1(1), of “making the use of internet services regulated by this Act safer for individuals in the United Kingdom”	

Our main concerns with the overall approach are as follows:

1) A "first iteration" doesn't have to be such an unambitious iteration

Ofcom has indicated, in both the consultation and in other communications, that it sees its proposed measures as a "first iteration", which it expects to expand on in the coming years through quite frequent iterations. But whilst we agree with an iterative approach, we do not think it justifies Ofcom's decision to set the bar so very low in its first iteration. Ofcom appears to intend to "iterate up", from this low bar – and has therefore erred on the side of not recommending measures which have the potential to prevent harm where it perceives there to be evidential gaps, or where it perceives uncertainty as to the capacity of companies to comply with a measure.

This approach amounts to prioritising the interests of regulated companies over users. We are not sure which part of the Act Ofcom considers to require it to steer it towards applying a precautionary principle to avoid inconveniencing companies, rather than applying a precautionary principle to protect users from illegal harms. Our view is that it is clear from the legislation itself, and the parliamentary discussions surrounding it, that user safety was expected to take precedence, erring on the side of recommending what appears necessary to tackle illegal harms, but with the ability to relax measures should they later prove to be unnecessary or have been overtaken by developments.

An absence of evidence should not be treated as evidence against a measure. The default response to an imperfect evidence base should not be to reject recommendations, and consequently to leave huge unaddressed risks in the package of proposed measures. Rather Ofcom should look to fill those evidentiary gaps, if indeed they exist, but in the meantime recommend measures which, on the balance of probabilities based on the evidence it has at its disposal, are likely to help protect users from the risks it has identified. If evidence subsequently emerges which challenges the effectiveness of a measure, then that measure can be revisited and potentially removed or relaxed in a later iteration.

2) An incomplete package of recommendations is inconsistent with the requirements of Section 41(1) of the Act

We note Ofcom's recognition that "services that decide to implement measures recommended to them for the kinds of illegal harms and their size or level of risk indicated in our Codes of Practice will be treated as complying with the relevant duty. This means that Ofcom will not take enforcement action against them for breach of that duty." This closely follows the language of s41(1) of the Act.

This "safe harbour" provision makes it all the more critical that, from its very first iteration, Ofcom recommends a comprehensive set of measures to address the full range of risks and harms it has identified in its risk register. The measures need to be sufficient to deliver the improvement in online safety which is the purpose of the Act. It is manifestly not the intent of S41(1) for a platform with a continued high prevalence of illegal harm to enjoy a "safe harbour", simply because they've followed an insufficiently stringent set of measures.

In other words, s41(1) requires Ofcom to be confident that its measures are sufficiently stringent to fulfil the Act's stated purpose of ensuring that companies "identify, mitigate and manage the risks of harm" and that their platforms are "safe by design". It has to be obvious that the "safe harbour" was only intended by the legislators to be available in circumstances in which the measures and recommendations clearly satisfied the aims of the legislation in terms of reducing harms.

3) Following Ofcom's "measures" don't have to mean a tick-box exercise for platforms

There are places where Ofcom could and should have recommended an additional specific measure to address a specific harm or risk factor. One of the most significant omissions of this sort is recommending a measure to address the numerous risks which Ofcom has identified with anonymous and fake profiles. We have included, as a separate document, a detailed proposal for a measure requiring platforms to offer their users options to verify their identity.

However, the Act offers a broad definition of "measure", in sections 10(4) and 236(1), which would allow Ofcom in addition to make recommendations which put more onus on platforms to take their own share of responsibility for identifying and implementing specific steps to reduce specific risks generated by their services. We would propose that Ofcom includes in its list of recommended measures processes that platforms must follow to identify, implement, and evaluate actions designed to address the specific risks arising from the design and functionality of their particular service, as identified in their risk assessments.

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

No

Enhanced user control (U2U)

Question 37:

i) Do you agree with our proposals?

Yes, as far as they go

ii) Please provide the underlying arguments and evidence that support your views.

We strongly agree that giving users options to block and mute other users, and to disable comments, can help protect them against a range of harms, and it makes sense to recommend platforms to offer these functionalities.

As you note, "the effectiveness of individual blocking tools may be limited in circumstances where the blocked user creates new accounts through which to continue targeting the blocking user". We therefore suggest the blocking and muting measures would be much more effective if combined with a measure offering users options to verify their identity, combined with an option to mute or block non-verified users as a category. This would make it much harder for a blocked user to circumvent a block to continue their illegal behaviour by creating new accounts, and mean that targeted users would have an option to block all non-verified accounts rather than being forced to play "whack-a-mole".

We refer you to our attached document, “Proposal for the inclusion, in the Illegal Harms Codes of Practice, of a measure requiring platforms to offer their users options to verify their identity”, which sets this out in detail.

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

No

Question 38:

i) Do you think the first two proposed measures should include requirements for how these controls are made known to users?

Yes. With any user control measure, users being aware of the functionality’s existence, how it could help them, and how to use it, is critical.

There is a risk that platforms do not see take up of these measures as desirable as they may lower user engagement and therefore ad revenue. Platforms should therefore be required to take reasonable steps to ensure that users are aware of these functionalities and how to use them, and to conduct periodic assessments of user awareness and user take-up.

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

No

Question 39:

i) Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?

Making users aware of the distinctions between “notable” and “monetised” verification schemes is a limited, but positive, proposal. It will be of particular value where there is a discrepancy between the level of rigour applied as between a notable scheme and the “monetised” schemes, which makes any confusion between the two schemes easier for an impersonation scammer to exploit.

It would make sense for Ofcom to also, within this proposed measure, set some minimum standards for any scheme describing itself as “verification”, to avoid scenarios, such as those which arose with “Twitter Blue”, where bad actors could easily obtain the credibility of a “blue tick” without going through any form of meaningful verification at all beyond making an online payment. We explored the risks of this approach here.

We do not, however, think these proposed measures are anywhere near sufficient to address the risks associated with anonymous and fake accounts, as identified by Ofcom in its Register of Risks. The Register of Risks identifies anonymous and/or fake accounts as a “stand out” risk factor, linked to a considerable number of serious harms: Terrorism; Grooming; CSAM; Suicide and Self-Harm; Harassment, stalking, threats and abuse; Hate offences; Drugs offences; Firearms offences; Extreme pornography; Intimate image abuse; Fraud; Foreign Interference offence; False communications offence; Epilepsy trolling; Cyberflashing. The proposed measure on “notable” and “mon-

etised" verification schemes only aims to mitigate the risks of one subset of fake accounts, in order to address one subset of one of these 15 offences (fraud relying on impersonation of a notable figure). Whilst we agree with Ofcom's decision not to recommend a *mandatory* user identity verification measure, which it explores in this section, we strongly disagree with the decision to not go on to consider recommending a *voluntary* user verification measure under the illegal content codes. We have been encouraged, in meetings with Ofcom staff, to set out a detailed proposal for how a measure requiring platforms to offer their users options to choose to verify their identity, alongside clear labelling of which accounts are, and are not, verified, and options to mute and block non-verified accounts, might work. We are appending this as a separate document, titled "Proposal for the inclusion, in the Illegal Harms Codes of Practice, of a measure requiring platforms to offer their users options to verify their identity". We would encourage you to include a recommendation of this measure in this first iteration of the codes of practice, to avoid leaving largely unaddressed the very significant risks of illegal harms associated with anonymous and fake accounts, which Ofcom has itself identified.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No	

Cumulative Assessment

Question 45:	
i)	Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?
Unsure	
ii)	Please provide the underlying arguments and evidence that support your views.
We have serious concerns about how Ofcom is choosing to define proportionality. An overall methodology for assessing proportionality is not described, and there appears to be too much focus on costs to businesses, with insufficient consideration of the significant costs to society and harms to individual users of failing to recommend sufficiently stringent measures.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No	

Question 46:	
i)	Do you agree that the overall burden is proportionate for those small and micro businesses that find they have significant risks of illegal content and for whom we propose to recommend more measures?
Unsure	

ii) Please provide the underlying arguments and evidence that support your views.

As stated in our previous answers, we have reservations about how Ofcom appears to be defining proportionality, and concerns that Ofcom's recommendations may not, taken together, do much to improve online safety.

That said, we think it is entirely appropriate for businesses which have more risks to be required to take more measures to address those risks. We do not see in the Act any suggestion that platforms which pose serious risks should escape the Act merely on account of their small size.

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

Question 47:

i) We are applying more measures to large services. Do you agree that the overall burden on large services is proportionate?

Unsure

ii) Please provide the underlying arguments and evidence that support your views.

Again, we are concerned that Ofcom's approach to what is proportionate appears to be unduly focused on minimising costs to companies, rather than safety of users, and that "proportionate" seems to act as a synonym for "light touch". We would agree that the proposed measures are indeed very light touch.

We think a better definition of proportionate would mean that the measures were sufficient to accomplish the safety objectives of the Act, and tackle the harms and risks identified in the Register of Risks. We cannot see how the package of measures for large and high risk services will tackle the risks and harms identified in Ofcom's Register of Risks, so we wouldn't describe the measures as proportionate. We are submitting a detailed proposal for one additional measure, which would help address the risks associated with fake and anonymous accounts.

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

Statutory Tests

Question 48:

i) Do you agree that Ofcom's proposed recommendations for the Codes are appropriate in the light of the matters to which Ofcom must have regard?

No

ii) Please provide the underlying arguments and evidence that support your views.

We do not see how, taken together, Ofcom's proposed recommendations will deliver on the Act's overall purpose of improving online safety. This has huge implications for human rights of law-abiding users of platforms, whose privacy, freedom of expression, and other human rights may be negatively affected by encountering or being targeted with illegal content.

We are concerned that Ofcom has placed too much emphasis on rights of certain users whose speech or reach might be impacted by a measure under consideration, and not done enough to balance this against the rights of other users (including victims of serious crimes) who are impacted by the illegal harms that the measure has the potential to prevent.

For example, in its consideration of anonymity Ofcom correctly notes that anonymity can be a feature which is valued by vulnerable or minoritised groups, but fails to note that these same groups are often disproportionately affected by the harms associated with anonymous and fake accounts, or that being targeted in this way can itself have a significant chilling effect on a user's freedom of expression.

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

No