CLEAN UP THE INTERNET

Submission to the "Online Harms White Paper" consultation

1st July, 2019

What is the name and address of the organisation or interest group you represent?

Clean Up The Internet

10 Queen Street Place,

London

EC4R 1BE

What sector best describes the organisation or interest group you represent?

Not-for-profit, civil society

Contact:

Clean Up the Internet – contact@cleanuptheinternet.org.uk

Please describe the organisation or interest group you represent and its activities

Clean up the Internet is a recently formed organisation, concerned about the harmful impact the twin scourges of online abuse and disinformation are having on our society. We are pleased to have the opportunity to respond to the Online Harms White Paper.

Clean up the Internet shares the government's overall goals and would be pleased to provide further support and assistance in order to ensure the UK becomes a global example for how to create a safe and trustworthy internet.

The following sets out our initial responses to the questions included in the White Paper. We have only answered the questions where we have relevant views and expertise.

Question 1*: This government has committed to annual transparency reporting. Beyond the measures set out in this White Paper, should the government do more to build a culture of transparency, trust and accountability across industry and, if so, what?*

This first Question provides an appropriate opportunity to outline our key concern. We welcome the measures set out in the White Paper, and the desire to establish "rules and norms for the internet that discourage harmful behaviour". However we think that in 3.17 of the White Paper there is currently insufficient consideration given to measures that would reduce the negative impacts of anonymous participation on social media platforms and on the comment pages of newspapers. We strongly believe that the regulator should require companies to report on their approach to managing the challenges associated with anonymity and account verification, and that a requirement to manage anonymity and user verification should be included in the duty of care

It is essential to recognise that anonymity is widely accepted as a significant factor in harmful behaviour online, and one which undermines transparency, trust and accountability. For example the DCMS paper *Rapid Evidence Assessment: The Prevalence and Impact of Online Trolling* notes "the 'Gyges effect' or 'Online Disinhibition Effect' –the idea that anonymity seemingly lowers self-awareness and inhibition, whilst encouraging a dissociation from the harassment, which has received robust empirical support".

The White Paper rightly acknowledges that some media platforms have "become akin to public spaces", and that the quality and nature of the discourse which takes place on them has a significant bearing on the health of our democracy. Yet we would not as a rule, in our physical public spaces, encourage individuals to don masks and then harangue each other. It is therefore appropriate to consider what limitations should be placed on the ability of anonymous users to intervene and influence these online public spaces.

The White Paper highlights, for example, the abuse of public figures on Twitter. It quotes Rachel Maclean MP describing "anonymous people that you've never met...the hatred and bile they are directing towards you." A Home Affairs Select Committee's April 2017 report on hate crime noted that MPs experience "high levels of racism, misogynistic abuse and other forms of harassment on Twitter" and that this disproportionately targeted female and ethnic minority MPs.

The chilling effect of online abuse extends well beyond MPs and other public figures. Research conducted by Amnesty International in 2017 found that 1 in 3 women in the UK reported having changed the way they express themselves online in response to abuse or harassment. At present anonymous, pseudonymous and unverified twitter users are free to derail debates with abusive or misleading comments, and to create an online environment where female, BAME and LGBTQ+ users are more likely to feel intimidated or silenced.

As well as anonymity having a disinhibiting effect on individual bad behaviour, and creating an intimidating environment for other users, it also makes it impossible for sites to enforce their existing Terms of Use. The White Paper notes the problem of "banned users creating new accounts" to continue breaking the rules, and anticipates the regulator producing guidance on ways to tackle this in a future code of practice. We believe that in reality it will be very difficult to make progress on this issue without first tightening up rules around anonymity, and that this should therefore be made an early priority. Users will take Terms of Use and Codes of Conduct more seriously if they are reminded of them at the same point as they are required to verify their identity. This will make them more likely to abide by those codes, and more likely to challenge or report infringements by others.

There are many ways of tackling the challenges associated with anonymity and disinhibition, and we are not wedded to a particular solution. The test of any approach should be that it meets the overall objective of improving behaviour and the quality of online debate, and reducing other users' exposure unsolicited harassment, bullying, intimidation or misinformation. What is clear is that where a site or network is "akin to a public space", a shift away from the current lack of restrictions on anonymous, pseudonymous and unverified use is urgently required. The regulator should regard this as a key feature of sites making themselves "safe by design" and require companies to explain how they are addressing it. This has the additional benefit of being a more efficient approach. It will generally take far less resource to address this underlying factor which leads to harmful, abusive or inaccurate content being posted than it will to police content effectively once it has been posted.

Systems of verification could require a user to provide credit card or other personal details, in exchange for which they could be given "trusted user" status allowing them to participate in public forums and discussions initiated by others, and to make unsolicited responses to others. In the case of Twitter, potential measures could include extending the "verified account" programme, to enable any user to verify their identity, placing restrictions on unverified users' ability to make unsolicited contact, and enabling all users to easily block or filter all content from unverified accounts by category with a single action, rather than having to individually block multiple accounts. However we would urge against reliance upon measures that place too much emphasis on actions needing to be taken by the "victims", rather than tackling the behaviour of the perpetrators.

It may not be necessary to insist that the user is individually identifiable to everyone who is exposed to their comments, as long as they have sufficiently identified themselves to the network or platform so that they would be deterred from abusing that position. If a company is able to demonstrate to the regulator that this is proving effective for a given platform, then that should be considered an acceptable approach.

There are of course circumstances in which anonymity is very important and should be protected. We would not want to deter a whistle-blower from releasing materials from the safety of an unidentified account or stop a commentator posting to his/her followers. We want to stress that our proposals would seek to limit only the circumstances in which an anonymous user can intervene into conversations started by others or send unsolicited communication. We would not support restrictions on anonymity for someone publishing unilaterally on their own "site", or tweeting to their own followers.

We also recognise that limitations on anonymity which would be beneficial in the United Kingdom, where we have strong legal protections for freedom of expression, and for whistle blowing, might have a chilling effect in some other parts of the world. But here in the UK the current lack of regulation with regard to anonymity is contributing to online harm, and we should develop a proportionate regulatory approach in line with our democratic norms and values.

***Question 2**: Should designated bodies be able to bring 'super complaints' to the regulator in specific and clearly evidenced circumstances?*

We are not at this stage convinced that it is necessary to entrust functions to another layer of organisations that could have the unintended effect of disempowering individual users. Moreover, placing emphasis on the ability to complain involves focusing on cure, whereas we are more interested in engaging first in steps that will deter or prevent harms, and therefore make redress less necessary. Nevertheless, and accepting that some mechanisms for redress will be needed, if any representative body were to bring together a large number of complaints, those should attract the weight and attention that they deserve. But we would be cautious about creating another set of gatekeepers to the overriding goal of making the internet a safer and more productive space.

***Question 3**: What, if any, other measures should the government consider for users who wish to raise concerns about specific pieces of harmful content or activity, and/or breaches of the duty of care?*

The government should ensure that companies implement user-friendly redress mechanisms. In the case of a company's systemic failure to address justified complaints, the user should be able to contact the regulator or designated body, equally in a user-friendly manner. Nevertheless, we believe that the emphasis of the regulatory framework should be on making companies behave more responsibly rather than ex-post measures. Efforts from designated bodies and regulator should however primarily be focused at larger platforms that bring serious numbers of users together. The government is right to consider scale in this context.

***Question 4**: What role should Parliament play in scrutinising the work of the regulator, including the development of codes of practice?*

As long as the direction that is given is clear, and the regulator has sufficiently qualified and motivated staff as well as resources, it ought to be possible for Parliament to supervise with a light touch and to give clear guidance on the codes of practices and what is expected from companies that fall within the scope of the regulatory framework.

We assume that the regulator would report to the Department of Digital, Culture, Media & Sport and be required to appear before the Digital, Culture, Media and Sport Committee on a regular basis, which might initially be relatively frequent in the start-up phase but then probably require no more than one or two sessions per year.

***Question 5**: Are proposals for the online platforms and services in scope of the regulatory framework a suitable basis for an effective and proportionate approach?*

We do not question their suitability per se, and we see them as a necessary if not a sufficient first step, but we believe additional attention should be paid to the problems associated with anonymity.

***Question 8**: What further steps could be taken to ensure the regulator will act in a targeted and proportionate manner?*

The regulator should be easily accessible, be held accountable and hold regular forums, both in person and online, in which it receives feedback and also explains its action or inaction. Given that similar measures are being considered or implemented in other EU Member States, lawmakers should try to take this into account as much as possible to ensure a certain level of legal harmonisation for companies, in particular smaller ones. And such consistency of approach will, in the online world, be necessary whatever course Brexit takes.

***Question 9**: What, if any, advice or support could the regulator provide to businesses, particularly start-ups and SMEs, comply with the regulatory framework?*

It will be necessary for the regulator to be well-enough resourced, confident and able to contact businesses quickly and encourage them to bring themselves into compliance. We would hope that the regulatory framework and/or duties of care would be sufficiently clear and principle-based, hence limiting the need for guidance. Nevertheless, bearing in mind the limited financial means and resource of start-ups and SMEs, it will be important for the regulator to provide these companies with best practices, additional guidance and avoid excessive burden as explained in Box 26 of the White Paper.

***Question 10**: Should an online harms regulator be: (i) a new public body, or (ii) an existing public body?*

We would have reservations, at least initially, about creating a new body. If regulation is to be effective from the start it is probably best entrusted to an existing body with experienced staff and the confidence to take enforcement action. We would also not wish to see conflicts or jurisdictional gaps between overlapping or concurrent bodies, as has happened in other areas.

***Question 10a**: If your answer to question 10 is (ii), which body or bodies should it be?*

In principle we are relatively agnostic as to which body should take responsibility for this initiative, but given our comments in response to Question 10, we can see great benefit initially in an existing body such as Ofcom. However, should that be the decision, Ofcom's mandate would need to be expanded and it be allocated the resources and staff to enforce the new regulatory framework. We also envisage that Ofcom would need to be supported and guided by an Advisory Panel composed of a range of stakeholder representatives.

***Question 11**: A new or existing regulator is intended to be cost neutral: on what basis should any funding contributions from industry be determined?*

It is difficult to answer this question in isolation, without having any idea of what the costs are expected to be. Consistent with what we have said earlier, if the regulation (at least with respect to our concerns over misuse of anonymity) is principle-based and puts clear obligations on the channels, and if it is clear that intervention will be swift and decisive, we do not see why this should require an oppressive financial burden upon industry. We would like to see a "smart" approach to burden sharing, which could initially be based on a simple yardstick such as user base and/or revenues, but which rapidly could introduce the concept of a "no claims bonus" for those channels who do not require much intervention.

***Question 12**: Should the regulator be empowered to i) disrupt business activities, or ii) undertake ISP blocking, or iii) implement a regime for senior management liability? What, if any, further powers should be available to the regulator?*

We strongly believe that the regulator should have the full range of powers necessary to intervene swiftly and to give platforms the correct incentives to comply. As this proposal advances we would be happy to assist with suggestions and a draft enforcement scheme.

***Question 13**: Should the regulator have the power to require a company based outside the UK and EEA to appoint a nominated representative in the UK or EEA in certain circumstances?*

We are concerned at the ability of certain businesses to avoid jurisdiction by disputing or shifting the location from which they are managed and therefore would agree that it should be a condition of being allowed to do business in the UK, including communicating with and selling adverts to UK citizens, that companies should have taken practical steps to accept jurisdiction and make themselves subject to effective enforcement. This is likely to become even more important post-Brexit if we find ourselves outside current mechanisms for mutual recognition and enforcement.

***Question 14**: In addition to judicial review should there be a statutory mechanism for companies to appeal against a decision of the regulator, as exists in relation to Ofcom under sections 192-196 of the Communications Act 2003?*

We are not convinced that judicial review is an appropriate or efficient mechanism. Moreover, the question concentrates only on appeals by companies, whereas we would expect citizens and those who represent them also to be able to appeal against rulings that do not satisfy them. Those appeals should be on substance rather than merely challenging adherence to some administrative standard. We would wish to see a simple fast track review system with a minimum of procedural input. Given that the disputes will mostly by definition be fact rather than law based, we would urge the adoption of an expert-led redress mechanism that minimises legal input and costs.

***Question 17**: Should the government be doing more to help people manage their own and their children's online safety and, if so, what?*

We highlighted in question 1 that we think more can be done to tackle the misuse of anonymity. We believe that this would have significant benefits in terms of online safety, including by:

- reducing the impact of the "online disinhibition effect" as a cause of bad behaviour

- creating a more transparent and trusted environment for all users

- making it easier for sites to enforce Terms of Use including permanent bans, and applying those bans beyond a single platform

- restricting the ability of anonymous or fake accounts to target and interact with all persons, including vulnerable adults and children

- limiting the dissemination of disinformation and fake news by unaccountable actors

***Question 18**: What, if any, role should the regulator have in relation to education and awareness activity?*

The regulator should issue regular updates, easily available and communicated directly to the public, in order to raise awareness and educate. In addition, there may be opportunities for the regulator to engage directly with the public through the education system and/or other public forums.