Written evidence submitted by Clean up the internet (OSB0239)

Alternative proposals for tackling anonymous abuse

Our recommendations (explicitly define anonymity as a risk-factor which platforms are required to act to mitigate; introduce specific requirements for platforms to offer their users a "right to verify", a "right to block interaction from unverified accounts", and for transparency about the verification status of all users)
seek to strike a balance that recognises and minimises the trade-offs involved in seeking to tackle the harms associated with anonymous accounts.

Below we discuss two other approaches which have been suggested and highlight some key advantages and disadvantages. A key distinction between these approaches and our own is that whereas we propose to offer users more choices to control their social media experience, these alternative proposals rely more greatly on compulsion. This raises questions of proportionality. It also places an even higher premium on ensuring that verification processes are accessible, including to those who are vulnerable or with complex identification circumstances – given that if verification is made compulsory an inability to complete verification would exclude them from social media altogether.

a) Make verification compulsory for all social media users

This proposal would require social media users to adopt a "know your user" approach for anyone using their platform. This could be coupled with vicarious liability for platforms were they unable to identify an end user.

The main advantage of this approach would be that it could entirely eliminate the problems associated with anonymous accounts - because it would entirely eliminate anonymity. In the case of criminal or defamatory activity it would ensure full traceability. It would also have the potential to provide a simpler user experience, by avoiding any scope for confusion amongst users about different verification statuses or the need for any user action to manage their level of interaction with unverified accounts (because there
wouldn't be any unverified accounts).

The main risk would be that it would eliminate legitimate uses of anonymity alongside eliminating its misuse. This would have implications for freedom of expression, so careful consideration would need to be given as to whether this was a proportionate intervention.

The negative implications for freedom of expression would be particularly significant were verification processes not fully accessible. Compulsory verification would therefore place a particularly high premium on ensuring that verification worked for vulnerable groups including those with more complex identification needs or lacking access to standard documentation.

b) Require users to verify their identities to social media platforms, but allow users to remain incognito toother users

This approach would entail users providing identifying information to a platform, which the platform could retain against their account, but not sharing this with other users to whom they could remain anonymous or use a pseudonym. The platform would be obliged to make this identifying information available to law enforcement, and in the case of defamation proceedings. It would also be able to use it to enforce its terms and conditions more effectively by preventing users evading suspensions through the creation of a new account.

The principal advantage of this approach would be that it would potentially lower the bar to verification, by making it palatable to users who had concerns about other users identifying them (e.g. because they didn't want an employer or their family to be able to identify them) but did not have qualms about being identifiable to a platform. This could potentially increase the uptake of verification - or if made mandatory, maintain scope for certain forms of benign anonymous (to other users) activity.

A major disadvantage would be that it would do less to increase trust, authenticity, or accountability in digital spaces because large numbers of users would remain anonymous to each other. Users would be traceable in criminal cases but could remain anonymous for purposes of non-criminal trolling or bullying. There would therefore be less of a reduction in the "online disinhibition effect".

Another disadvantage would be that it would centralise more information in the hands of platforms, rather than distributing more information and accountability amongst users. This data would need to be retained for as long as a user had an account with the platform, creating a new centralised dataset held by platforms, which could have privacy and security implications. An approach which verified publicly declared identity information would avoid such issues as verification of a public profile could easily be provided by a third party, and there would be no need for any extra personal data to be retained by the platform once verification has been completed. And whilst traceability data would exist, law enforcement agencies would remain dependent on platforms to disclose this data, and victims of defamation would continue to rely on Norwich Pharmacal orders to determine the identity of a user sharing defamatory content.